

ELECTRONIC COUPON SYSTEM AND METHOD FOR ISSUING AND VERIFYING ELECTRONIC COUPON

Patent Number: JP11328269
Publication date: 1999-11-30
Inventor(s): UMEZAWA KATSUYUKI; SUZAKI SEIICHI; YOSHIURA YUTAKA; TOYOSHIMA HISASHI; SAITO TSUKASA
Applicant(s): HITACHI LTD
Requested Patent: ☐ JP11328269
Application Number: JP19980133550 19980515
Priority Number (s):
IPC Classification: G06F17/60; G07F7/08; G07G1/12; G09C1/00; H04L9/32
EC Classification:
Equivalents:

Abstract

PROBLEM TO BE SOLVED: To detect forgery and alteration of a coupon and the illegal use of a coupon by a third person even when the coupon electronically issued is printed and used.

SOLUTION: It is possible to detect alteration and forgery of a coupon by verifying a digital signature described on the coupon even when a consumer 200 prints a coupon and uses it because a seller 100 produces a coupon on which the irreversible conversion value of a password transmitted from the consumer 200, coupon information that makes trouble if it is altered and a digital signature of the coupon information are described as visually recognizable data even when it is printed at the time of issuing the coupon. Also, it is possible to detect illegal use of a coupon by a third person by such manners that the consumer 200 presents the same password as at the time of being issued when the consumer uses it and that the seller 100 compares the irreversible conversion value of the presented password with an irreversible conversion value described on the coupon.

(19) 日本国特許庁 (J P)

(12) 公開特許公報 (A)

(11) 特許出願公開番号

特開平11-328269

(43) 公開日 平成11年(1999)11月30日

(51) Int.Cl. ⁸	識別記号	F I	
G 0 6 F 17/60		G 0 6 F 15/21	Z
G 0 7 F 7/08		G 0 7 G 1/12	3 2 1 M
G 0 7 G 1/12	3 2 1	G 0 9 C 1/00	6 6 0 Z
G 0 9 C 1/00	6 6 0	G 0 7 F 7/08	M
H 0 4 L 9/32		H 0 4 L 9/00	6 7 5 C
審査請求 未請求 請求項の数18 O L (全 35 頁)			

(21) 出願番号 特願平10-133550

(22) 出願日 平成10年(1998) 5月15日

(71) 出願人 000005108

株式会社日立製作所

東京都千代田区神田駿河台四丁目 6 番地

(72) 発明者 梅澤 克之

神奈川県川崎市麻生区王禅寺1099番地 株

式会社日立製作所システム開発研究所内

(72) 発明者 洲崎 誠一

神奈川県川崎市麻生区王禅寺1099番地 株

式会社日立製作所システム開発研究所内

(72) 発明者 吉浦 裕

神奈川県川崎市麻生区王禅寺1099番地 株

式会社日立製作所システム開発研究所内

(74) 代理人 弁理士 富田 和子

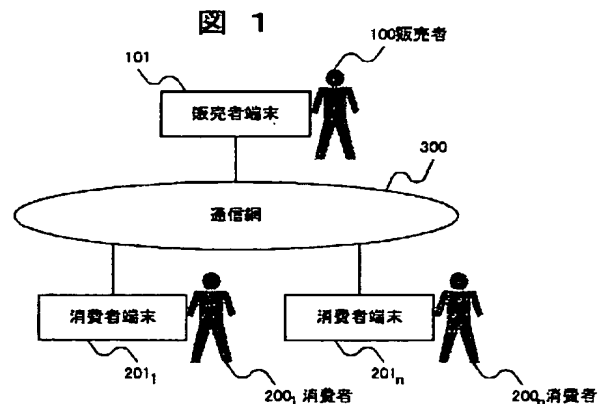
最終頁に続く

(54) 【発明の名称】 電子クーポンシステムおよび電子クーポン発券・検証方法

(57) 【要約】

【課題】 電子的に発券されたクーポンを印刷して使用する場合でも、クーポンの偽造や改ざん、第三者によるクーポンの不正使用を検出することを可能とする。

【解決手段】 クーポン発券時に、販売者100は、消費者200から送信されたパスワードの不可逆変換値と、改ざんされては困るクーポン情報と、クーポン情報のデジタル署名とを、印刷しても目視可能なデータとして記載したクーポンを作成するので、消費者200がクーポンを印刷して使用する場合でも、クーポンに記載されているデジタル署名を検証することで、クーポンの改ざんや偽造を検出することができる。また、消費者200は、クーポンの使用時に、発券時と同じパスワードを販売者100に提示し、販売者100は、提示されたパスワードの不可逆変換値と、クーポンに記載されている不可逆変換値とを比較することで、第三者によるクーポンの不正使用を検出することができる。



【特許請求の範囲】

【請求項1】消費者が利用する少なくとも1つの消費者端末と、販売者が利用する少なくとも1つの販売者端末とが、ネットワークを介して相互に接続されてなり、上記消費者端末は、上記販売者端末に対して、消費者のパスワードを送信して、1枚で予め定めた効力を発揮するクーポンの発券を要求するクーポン発券要求手段と、上記販売者端末から送信されてくるクーポンを受信するクーポン受信手段と、上記販売者端末に対して、消費者のパスワードと、上記クーポン受信手段が受信したクーポンとを送信して、該クーポンの使用を要求するクーポン使用要求手段と、上記クーポン受信手段が受信したクーポンを印刷するクーポン印刷手段とを備え、上記販売者端末は、上記消費者端末から発券が要求されたクーポンを、該消費者端末に対して送信するクーポン発券手段と、上記消費者端末から送信されて使用が要求されたクーポン、および、上記消費者端末で印刷されて使用が要求されたクーポンを検証するクーポン検証手段とを備え、上記販売者端末のクーポン発券手段は、上記消費者端末から送信されてきたパスワードを受信し、受信したパスワードの不可逆変換値と、クーポンの効力に関するクーポン情報と、該クーポン情報を、販売者だけしか知らない秘密の暗号鍵を用いて暗号化した暗号化情報とを、目視可能なデータとして記載したクーポンを作成し、作成したクーポンを該消費者端末に対して送信し、上記販売者端末のクーポン検証手段は、上記消費者端末から送信されて使用が要求されたクーポンを検証する場合に、該消費者端末から送信されてきたパスワードおよびクーポンを受信し、受信したパスワードの不可逆変換値と、受信したクーポンに記載されている不可逆変換値とが一致するか否かを検証すると共に、受信したクーポンに記載されているクーポン情報を、販売者だけしか知らない秘密の暗号鍵を用いて暗号化した暗号化情報と、受信したクーポンに記載されている暗号化情報とが一致するか否かを検証し、上記消費者端末で印刷されて使用が要求されたクーポンを検証する場合に、印刷されたクーポンに記載されている不可逆変換値とクーポン情報と暗号化情報とを取得し、消費者から提示されたパスワードの不可逆変換値と、取得した不可逆変換値とが一致するか否かを検証すると共に、取得したクーポン情報を、販売者だけしか知らない秘密の暗号鍵を用いて暗号化した暗号化情報と、取得した暗号化情報とが一致するか否かを検証することを特徴とする電子クーポンシステム。

【請求項2】消費者が利用する少なくとも1つの消費者端末と、販売者が利用する少なくとも1つの販売者端末とが、ネットワークを介して相互に接続されてなり、上記消費者端末は、上記販売者端末に対して、消費者のパスワードを送信して、1枚で予め定めた効力を発揮するクーポンの発券を要求するクーポン発券要求手段と、上記販売者端末から送信されてくるクーポンを受信するクーポン受信手段と、上記販売者端末に対して、消費者のパスワードと、上記クーポン受信手段が受信したクーポンとを送信して、該クーポンの使用を要求するクーポン使用要求手段と、上記クーポン受信手段が受信したクーポンを印刷するクーポン印刷手段とを備え、上記販売者端末は、上記消費者端末から発券が要求されたクーポンを、該消費者端末に対して送信するクーポン発券手段と、上記消費者端末から送信されて使用が要求されたクーポン、および、上記消費者端末で印刷されて使用が要求されたクーポンを検証するクーポン検証手段とを備え、上記販売者端末のクーポン発券手段は、上記消費者端末から送信されてきたパスワードを受信し、受信したパスワードの不可逆変換値と、クーポンの効力に関するクーポン情報とを連結し、連結した結果を、公開鍵暗号方式における販売者の秘密鍵を用いて暗号化したデジタル署名と、上記クーポン情報とを、目視可能なデータとして記載したクーポンを作成し、作成したクーポンを該消費者端末に対して送信し、上記販売者端末のクーポン検証手段は、上記消費者端末から送信されて使用が要求されたクーポンを検証する場合に、該消費者端末から送信されてきたパスワードおよびクーポンを受信し、受信したクーポンに記載されているデジタル署名を、公開鍵暗号方式における販売者の公開鍵を用いて復号した結果得られるパスワードの不可逆変換値と、受信したパスワードの不可逆変換値とが一致するか否かを検証すると共に、受信したクーポンに記載されているデジタル署名を、公開鍵暗号方式における販売者の公開鍵を用いて復号した結果得られるクーポン情報と、受信したクーポンに記載されているクーポン情報とが一致するか否かを検証し、上記消費者端末で印刷されて使用が要求されたクーポンを検証する場合に、印刷されたクーポンに記載されているクーポン情報とデジタル署名とを取得し、取得したデジタル署名を、公開鍵暗号方式における販売者の公開鍵を用いて復号した結果得られるパスワードの不可逆変換値と、消費者から提示されたパスワードの不可逆変換値とが一致するか否かを検証すると共に、取得したデジタル署名を、公開鍵暗号方式における販売者の公開鍵を用いて復号した結果得

られるクーポン情報と、取得したクーポン情報とが一致するか否かを検証することを特徴とする電子クーポンシステム。

【請求項3】請求項1または2記載の電子クーポンシステムであって、

上記販売者端末のクーポン発券手段は、作成したクーポンと共に、公開鍵暗号方式における販売者の秘密鍵を用いて該クーポン全体を暗号化したデジタル署名を、上記消費者端末に対して送信し、

上記消費者端末のクーポン受信手段は、受信したクーポンと、該クーポンと共に送信されてきたデジタル署名を、公開鍵暗号方式における販売者の公開鍵を用いて復号した結果とが一致するか否かを検証することを特徴とする電子クーポンシステム。

【請求項4】請求項1、2または3記載の電子クーポンシステムであって、

上記クーポン情報は、クーポンごとに固有のシリアル番号を含み、

上記販売者端末は、効力を発揮済みのクーポンに記載されているクーポン情報中のシリアル番号を記憶するシリアル番号記憶手段を備え、

上記販売者端末のクーポン検証手段は、検証対象のクーポンに記載されているクーポン情報中のシリアル番号を、上記シリアル番号記憶手段が記憶済みでないか否かを検証することを特徴とする電子クーポンシステム。

【請求項5】請求項1、2、3または4記載の電子クーポンシステムであって、

上記消費者端末は、上記販売者端末に対して、消費者のパスワードを送信して、予め定めた n ($n > 1$) 枚だけ集めたときに予め定めた効力を発揮するクーポン（以下、「チケット」と称す。）のうちの、1枚目のチケットの発券を要求する初期チケット発券要求手段と、

上記販売者端末に対して、消費者のパスワードと、発券済みのチケットのうちの最新のチケット（以下、「発券済み最新チケット」と称す。）を送信して、2枚目以降のチケットの発券を要求するチケット発券要求手段と、

上記販売者端末から送信されてくるチケットを受信して保存するチケット受信手段とを備え、

上記販売者端末は、上記消費者端末から発券が要求された1枚目のチケットを、該消費者端末に対して送信する初期チケット発券手段と、

上記消費者端末から発券が要求された2枚目以降のチケットを、該消費者端末に対して送信するチケット発券手段とを備え、

上記販売者端末の初期チケット発券手段は、

上記消費者端末から送信されてきたパスワードを受信し、受信したパスワードと、 n 枚のチケットの組を識別するために付与した固有の値（以下、「UID」と称す。）と、販売者だけしか知らない秘密の情報とを連結し、連結した結果の不可逆変換値 H_1 に基づいて、不可逆変換値 H_i ($1 \leq i < n$) の不可逆変換値 H_{i+1} を順次計算し、上記UIDおよび不可逆変換値 H_n を、1枚目のチケットとして、該消費者端末に対して送信し、

上記販売者端末のチケット発券手段は、上記消費者端末から送信されてきたパスワードおよび発券済み最新チケットを受信し、受信したパスワードと、受信した発券済み最新チケットのうちのUIDと、販売者だけしか知らない秘密の情報とを連結し、連結した結果の不可逆変換値 H_1 に基づいて、不可逆変換値 H_i ($1 \leq i < n$) の不可逆変換値 H_{i+1} を順次計算し、受信した発券済み最新チケットのうちの不可逆変換値 H_m ($1 \leq m \leq n$) と、不可逆変換値 H_1 とが一致したならば、 n 枚のチケットの発券を完了し、一致しないならば、上記UIDおよび不可逆変換値 H_{m-1} を、次のチケットとして、該消費者端末に対して送信することを特徴とする電子クーポンシステム。

【請求項6】請求項1、2、3または4記載の電子クーポンシステムであって、

上記消費者端末は、上記販売者端末に対して、消費者のパスワードを送信して、予め定めた n ($n > 1$) 枚だけ集めたときに予め定めた効力を発揮するクーポン（以下、「チケット」と称す。）のうちの、1枚目のチケットの発券を要求する初期チケット発券要求手段と、

上記販売者端末に対して、消費者のパスワードと、発券済みのチケットのうちの最新のチケット（以下、「発券済み最新チケット」と称す。）を送信して、2枚目以降のチケットの発券を要求するチケット発券要求手段と、

上記販売者端末から送信されてくるチケットを受信して保存するチケット受信手段とを備え、

上記販売者端末は、上記消費者端末から発券が要求された1枚目のチケットを、該消費者端末に対して送信する初期チケット発券手段と、

上記消費者端末から発券が要求された2枚目以降のチケットを、該消費者端末に対して送信するチケット発券手段とを備え、

上記販売者端末の初期チケット発券手段は、上記消費者端末から送信されてきたパスワードを受信し、受信したパスワードと、 n 枚のチケットの組を識別するために付与した固有の値（以下、「UID」と称す。）とを連結し、販売者だけしか知らない秘密の暗号鍵を用いて、連結した結果を暗号化した暗号化情報 H_1 を計算すると共に、計算した暗号化情報 H_1 に基づい

て、暗号化情報 H_i ($1 \leq i < n$) の暗号化情報 H_{i+1} を順次計算し、上記U I Dおよび暗号化情報 H_n を、1枚目のチケットとして、該消費者端末に対して送信し、上記販売者端末のチケット発券手段は、上記消費者端末から送信されてきたパスワードおよび発券済み最新チケットを受信し、受信したパスワードと、受信した発券済み最新チケットのうちのU I Dとを連結し、販売者だけしか知らない秘密の暗号鍵を用いて、連結した結果を暗号化した暗号化情報 H_1 を計算すると共に、計算した暗号化情報 H_1 に基づいて、暗号化情報 H_i ($1 \leq i < n$) の暗号化情報 H_{i+1} を順次計算し、受信した発券済み最新チケットのうちの暗号化情報 H_m ($1 \leq m \leq n$) と、暗号化情報 H_1 とが一致したならば、 n 枚のチケットの発券を完了し、一致しないならば、上記U I Dおよび暗号化情報 H_{m-1} を、次のチケットとして、該消費者端末に対して送信することを特徴とする電子クーポンシステム。

【請求項7】請求項1, 2, 3または4記載の電子クーポンシステムであって、

上記消費者端末は、

上記販売者端末に対して、消費者のパスワードを送信して、予め定めた n ($n > 1$) 枚だけ集めたときに予め定めた効力を発揮するクーポン（以下、「チケット」と称す。）のうちの、1枚目のチケットの発券を要求する初期チケット発券要求手段と、

上記販売者端末に対して、消費者のパスワードと、発券済みのチケットのうちの最新のチケット（以下、「発券済み最新チケット」と称す。）とを送信して、2枚目以降のチケットの発券を要求するチケット発券要求手段と、

上記販売者端末から送信されてくるチケットを受信して保存するチケット受信手段とを備え、

上記販売者端末は、

上記消費者端末から発券が要求された1枚目のチケットを、該消費者端末に対して送信する初期チケット発券手段と、

上記消費者端末から発券が要求された2枚目以降のチケットを、該消費者端末に対して送信するチケット発券手段とを備え、

上記販売者端末の初期チケット発券手段は、

上記消費者端末から送信されてきたパスワードを受信し、受信したパスワードと、 n 枚のチケットの組を識別するために付与した固有の値（以下、「U I D」と称す。）と、1枚目のチケットである旨を示す枚数情報とを連結し、販売者だけしか知らない秘密の暗号鍵を用いて、連結した結果を暗号化した暗号化情報 H_1 を、1枚目のチケットとして、該消費者端末に対して送信し、

上記販売者端末のチケット発券手段は、

上記消費者端末から送信されてきたパスワードおよび発券済み最新チケットを受信し、受信した発券済み最新チ

ケットである暗号化情報 H_m ($1 \leq m \leq n$) を、販売者だけしか知らない秘密の暗号鍵を用いて復号した結果得られる枚数情報が、 n 枚目のチケットである旨を示す枚数情報であるならば、 n 枚のチケットの発券を完了し、そうでないならば、受信したパスワードと、受信した発券済み最新チケットである暗号化情報 H_m ($1 \leq m \leq n$) を、販売者だけしか知らない秘密の暗号鍵を用いて復号した結果得られるU I Dと、 $m+1$ 枚目のチケットである旨を示す枚数情報とを連結し、販売者だけしか知らない秘密の暗号鍵を用いて、連結した結果を暗号化した暗号化情報 H_{m+1} を、次のチケットとして、該消費者端末に対して送信することを特徴とする電子クーポンシステム。

【請求項8】請求項1, 2, 3, 4, 5, 6または7記載の電子クーポンシステムであって、

上記消費者端末は、

上記販売者端末に対してパスワードを送信する際には、公開鍵暗号方式における販売者の公開鍵を用いて該パスワードを暗号化してから送信し、

上記販売者端末は、

上記消費者端末から送信されてきたパスワードを受信した際には、公開鍵暗号方式における販売者の秘密鍵を用いて該パスワードを復号することを特徴とする電子クーポンシステム。

【請求項9】消費者が利用する少なくとも1つの消費者端末と、販売者が利用する少なくとも1つの販売者端末と、発券者が利用する少なくとも1つの発券者端末とが、ネットワークを介して相互に接続されてなり、

上記消費者端末は、

上記発券者端末に対して、消費者のパスワードを送信して、1枚で予め定めた効力を発揮するクーポンの発券を要求するクーポン発券要求手段と、

上記発券者端末から送信されてくるクーポンを受信するクーポン受信手段と、

上記販売者端末に対して、消費者のパスワードと、上記クーポン受信手段が受信したクーポンとを送信して、該クーポンの使用を要求するクーポン使用要求手段と、

上記クーポン受信手段が受信したクーポンを印刷するクーポン印刷手段とを備え、

上記発券者端末は、

上記消費者端末から発券が要求されたクーポンを、該消費者端末に対して送信するクーポン発券手段を備え、

上記販売者端末は、

上記消費者端末から送信されて使用が要求されたクーポン、および、上記消費者端末で印刷されて使用が要求されたクーポンを検証するクーポン検証手段を備え、

上記発券者端末のクーポン発券手段は、

上記消費者端末から送信されてきたパスワードを受信し、受信したパスワードの不可逆変換値と、クーポンの効力に関するクーポン情報と、該クーポン情報を公開鍵

暗号方式における発券者の秘密鍵を用いて暗号化したデジタル署名とを、目視可能なデータとして記載したクーポンを作成し、作成したクーポンを該消費者端末に対して送信し、

上記販売者端末のクーポン検証手段は、

上記消費者端末から送信されて使用が要求されたクーポンを検証する場合に、該消費者端末から送信されてきたパスワードおよびクーポンを受信し、受信したパスワードの不可逆変換値と、受信したクーポンに記載されている不可逆変換値とが一致するか否かを検証すると共に、受信したクーポンに記載されているデジタル署名を、公開鍵暗号方式における発券者の公開鍵を用いて復号した結果と、受信したクーポンに記載されているクーポン情報とが一致するか否かを検証し、

上記消費者端末で印刷されて使用が要求されたクーポンを検証する場合に、

印刷されたクーポンに記載されている不可逆変換値とクーポン情報とデジタル署名とを取得し、消費者から提示されたパスワードの不可逆変換値と、取得した不可逆変換値とが一致するか否かを検証すると共に、取得したデジタル署名を、公開鍵暗号方式における発券者の公開鍵を用いて復号した結果と、取得したクーポン情報とが一致するか否かを検証することを特徴とする電子クーポンシステム。

【請求項10】消費者が利用する少なくとも1つの消費者端末と、販売者が利用する少なくとも1つの販売者端末と、発券者が利用する少なくとも1つの発券者端末とが、ネットワークを介して相互に接続されてなり、

上記消費者端末は、

上記発券者端末に対して、消費者のパスワードを送信して、1枚で予め定めた効力を発揮するクーポンの発券を要求するクーポン発券要求手段と、

上記発券者端末から送信されてくるクーポンを受信するクーポン受信手段と、

上記販売者端末に対して、消費者のパスワードと、上記クーポン受信手段が受信したクーポンとを送信して、該クーポンの使用を要求するクーポン使用要求手段と、

上記クーポン受信手段が受信したクーポンを印刷するクーポン印刷手段とを備え、

上記発券者端末は、

上記消費者端末から発券が要求されたクーポンを、該消費者端末に対して送信するクーポン発券手段を備え、

上記販売者端末は、

上記消費者端末から送信されて使用が要求されたクーポン、および、上記消費者端末で印刷されて使用が要求されたクーポンを検証するクーポン検証手段を備え、

上記発券者端末のクーポン発券手段は、

上記消費者端末から送信されてきたパスワードを受信し、受信したパスワードの不可逆変換値と、クーポンの効力に関するクーポン情報とを連結し、連結した結果

を、公開鍵暗号方式における発券者の秘密鍵を用いて暗号化したデジタル署名と、該クーポン情報とを、目視可能なデータとして記載したクーポンを作成し、作成したクーポンを該消費者端末に対して送信し、

上記販売者端末のクーポン検証手段は、

上記消費者端末から送信されて使用が要求されたクーポンを検証する場合に、

該消費者端末から送信されてきたパスワードおよびクーポンを受信し、受信したクーポンに記載されているデジタル署名を、公開鍵暗号方式における発券者の公開鍵を用いて復号した結果得られるパスワードの不可逆変換値と、受信したパスワードの不可逆変換値とが一致するか否かを検証すると共に、受信したクーポンに記載されているデジタル署名を、公開鍵暗号方式における発券者の公開鍵を用いて復号した結果得られるクーポン情報と、受信したクーポンに記載されているクーポン情報とが一致するか否かを検証し、

上記消費者端末で印刷されて使用が要求されたクーポンを検証する場合に、

印刷されたクーポンに記載されているクーポン情報とデジタル署名とを取得し、取得したデジタル署名を、公開鍵暗号方式における発券者の公開鍵を用いて復号した結果得られるパスワードの不可逆変換値と、消費者から提示されたパスワードの不可逆変換値とが一致するか否かを検証すると共に、取得したデジタル署名を、公開鍵暗号方式における発券者の公開鍵を用いて復号した結果得られるクーポン情報と、取得したクーポン情報とが一致するか否かを検証することを特徴とする電子クーポンシステム。

【請求項11】請求項9または10記載の電子クーポンシステムであって、

上記発券者端末のクーポン発券手段は、

作成したクーポンと共に、公開鍵暗号方式における発券者の秘密鍵を用いて該クーポン全体を暗号化したデジタル署名を、上記消費者端末に対して送信し、

上記消費者端末のクーポン受信手段は、

受信したクーポンと、該クーポンと共に送信されてきたデジタル署名を、公開鍵暗号方式における発券者の公開鍵を用いて復号した結果とが一致するか否かを検証することを特徴とする電子クーポンシステム。

【請求項12】請求項9、10または11記載の電子クーポンシステムであって、

上記クーポン情報は、クーポンごとに固有のシリアル番号を含み、

上記発券者端末は、

上記販売者端末から通知されたシリアル番号を記憶するシリアル番号記憶手段と、

上記販売者端末から問い合わせがあったシリアル番号を、上記シリアル番号記憶手段が記憶済みでないか否かを検証し、検証結果を該販売者端末に対して回答するシ

リアル番号検証手段とを備え、
上記販売者端末のクーポン検証手段は、
効力を発揮済みのクーポンに記載されているクーポン情報中のシリアル番号を、上記発券者端末に対して通知すると共に、検証対象のクーポンに記載されているクーポン情報中のシリアル番号についての検証結果を、上記発券者端末に対して問い合わせることを特徴とする電子クーポンシステム。

【請求項13】請求項9、10、11または12記載の電子クーポンシステムであって、

上記消費者端末は、

上記発券者端末に対して、消費者のパスワードを送信して、予め定めた n ($n > 1$) 枚だけ集めたときに予め定めた効力を発揮するクーポン（以下、「チケット」と称す。）のうちの、1枚目のチケットの発券を要求する初期チケット発券要求手段と、

上記発券者端末に対して、消費者のパスワードと、発券済みのチケットのうちの最新のチケット（以下、「発券済み最新チケット」と称す。）を送信して、2枚目以降のチケットの発券を要求するチケット発券要求手段と、

上記発券者端末から送信されてくるチケットを受信して保存するチケット受信手段とを備え、

上記発券者端末は、

上記消費者端末から発券が要求された1枚目のチケットを、該消費者端末に対して送信する初期チケット発券手段と、

上記消費者端末から発券が要求された2枚目以降のチケットを、該消費者端末に対して送信するチケット発券手段とを備え、

上記発券者端末の初期チケット発券手段は、

上記消費者端末から送信されてきたパスワードを受信し、受信したパスワードと、 n 枚のチケットの組を識別するために付与した固有の値（以下、「UID」と称す。）と、発券者だけが知らない秘密の情報とを連結し、連結した結果の不可逆変換値 H_1 に基づいて、不可逆変換値 H_i ($1 \leq i < n$) の不可逆変換値 H_{i+1} を順次計算し、上記UIDおよび不可逆変換値 H_n を、1枚目のチケットとして、該消費者端末に対して送信し、

上記発券者端末のチケット発券手段は、

上記消費者端末から送信されてきたパスワードおよび発券済み最新チケットを受信し、受信したパスワードと、受信した発券済み最新チケットのうちのUIDと、発券者だけが知らない秘密の情報とを連結し、連結した結果の不可逆変換値 H_1 に基づいて、不可逆変換値 H_i ($1 \leq i < n$) の不可逆変換値 H_{i+1} を順次計算し、受信した発券済み最新チケットのうちの不可逆変換値 H_m ($1 \leq m \leq n$) と、不可逆変換値 H_1 とが一致したならば、 n 枚のチケットの発券を完了し、一致しないならば、上記UIDおよび不可逆変換値 H_{m-1} を、次のチケットと

して、該消費者端末に対して送信することを特徴とする電子クーポンシステム。

【請求項14】請求項9、10、11または12記載の電子クーポンシステムであって、

上記消費者端末は、

上記発券者端末に対して、消費者のパスワードを送信して、予め定めた n ($n > 1$) 枚だけ集めたときに予め定めた効力を発揮するクーポン（以下、「チケット」と称す。）のうちの、1枚目のチケットの発券を要求する初期チケット発券要求手段と、

上記発券者端末に対して、消費者のパスワードと、発券済みのチケットのうちの最新のチケット（以下、「発券済み最新チケット」と称す。）を送信して、2枚目以降のチケットの発券を要求するチケット発券要求手段と、

上記発券者端末から送信されてくるチケットを受信して保存するチケット受信手段とを備え、

上記発券者端末は、

上記消費者端末から発券が要求された1枚目のチケットを、該消費者端末に対して送信する初期チケット発券手段と、

上記消費者端末から発券が要求された2枚目以降のチケットを、該消費者端末に対して送信するチケット発券手段とを備え、

上記発券者端末の初期チケット発券手段は、

上記消費者端末から送信されてきたパスワードを受信し、受信したパスワードと、 n 枚のチケットの組を識別するために付与した固有の値（以下、「UID」と称す。）とを連結し、発券者だけが知らない秘密の暗号鍵を用いて、連結した結果を暗号化した暗号化情報 H_1 を計算すると共に、計算した暗号化情報 H_1 に基づいて、暗号化情報 H_i ($1 \leq i < n$) の暗号化情報 H_{i+1} を順次計算し、上記UIDおよび暗号化情報 H_n を、1枚目のチケットとして、該消費者端末に対して送信し、
上記発券者端末のチケット発券手段は、

上記消費者端末から送信されてきたパスワードおよび発券済み最新チケットを受信し、受信したパスワードと、受信した発券済み最新チケットのうちのUIDとを連結し、発券者だけが知らない秘密の暗号鍵を用いて、連結した結果を暗号化した暗号化情報 H_1 を計算すると共に、計算した暗号化情報 H_1 に基づいて、暗号化情報 H_i ($1 \leq i < n$) の暗号化情報 H_{i+1} を順次計算し、受信した発券済み最新チケットのうちの暗号化情報 H_m ($1 \leq m \leq n$) と、暗号化情報 H_1 とが一致したならば、 n 枚のチケットの発券を完了し、一致しないならば、上記UIDおよび暗号化情報 H_{m-1} を、次のチケットとして、該消費者端末に対して送信することを特徴とする電子クーポンシステム。

【請求項15】請求項9、10、11または12記載の電子クーポンシステムであって、

上記消費者端末は、
 上記発券者端末に対して、消費者のパスワードを送信して、予め定めた n ($n > 1$) 枚だけ集めたときに予め定めた効力を発揮するクーポン（以下、「チケット」と称す。）のうちの、1枚目のチケットの発券を要求する初期チケット発券要求手段と、
 上記発券者端末に対して、消費者のパスワードと、発券済みのチケットのうちの最新のチケット（以下、「発券済み最新チケット」と称す。）とを送信して、2枚目以降のチケットの発券を要求するチケット発券要求手段と、
 上記販売者端末から送信されてくるチケットを受信して保存するチケット受信手段とを備え、
 上記発券者端末は、
 上記消費者端末から発券が要求された1枚目のチケットを、該消費者端末に対して送信する初期チケット発券手段と、
 上記消費者端末から発券が要求された2枚目以降のチケットを、該消費者端末に対して送信するチケット発券手段とを備え、
 上記発券者端末の初期チケット発券手段は、
 上記消費者端末から送信されてきたパスワードを受信し、受信したパスワードと、 n 枚のチケットの組を識別するために付与した固有の値（以下、「UID」と称す。）と、1枚目のチケットである旨を示す枚数情報とを連結し、発券者だけが知らない秘密の暗号鍵を用いて、連結した結果を暗号化した暗号化情報 H_1 を、1枚目のチケットとして、該消費者端末に対して送信し、
 上記発券者端末のチケット発券手段は、
 上記消費者端末から送信されてきたパスワードおよび発券済み最新チケットを受信し、受信した発券済み最新チケットである暗号化情報 H_m ($1 \leq m \leq n$) を、発券者だけが知らない秘密の暗号鍵を用いて復号した結果得られる枚数情報が、 n 枚目のチケットである旨を示す枚数情報であるならば、 n 枚のチケットの発券を完了し、そうでないならば、受信したパスワードと、受信した発券済み最新チケットである暗号化情報 H_m ($1 \leq m \leq n$) を、発券者だけが知らない秘密の暗号鍵を用いて復号した結果得られるUIDと、 $m+1$ 枚目のチケットである旨を示す枚数情報とを連結し、発券者だけが知らない秘密の暗号鍵を用いて、連結した結果を暗号化した暗号化情報 H_{m+1} を、次のチケットとして、該消費者端末に対して送信することを特徴とする電子クーポンシステム。
 【請求項16】請求項9、10、11、12、13、14または15記載の電子クーポンシステムであって、
 上記消費者端末は、
 上記発券者端末に対してパスワードを送信する際には、公開鍵暗号方式における発券者の公開鍵を用いて該パスワードを暗号化してから送信し、また、上記販売者端末

に対してパスワードを送信する際には、公開鍵暗号方式における販売者の公開鍵を用いて該パスワードを暗号化してから送信し、
 上記発券者端末は、
 上記消費者端末から送信されてきたパスワードを受信した際には、公開鍵暗号方式における発券者の秘密鍵を用いて該パスワードを復号し、
 上記販売者端末は、
 上記消費者端末から送信されてきたパスワードを受信した際には、公開鍵暗号方式における販売者の秘密鍵を用いて該パスワードを復号することを特徴とする電子クーポンシステム。
 【請求項17】消費者が利用する少なくとも1つの消費者端末と、販売者が利用する少なくとも1つの販売者端末とが、ネットワークを介して相互に接続されてなるシステムにおいて、1枚で予め定めた効力を発揮するクーポンの発券および検証を行う方法であって、
 クーボンの発券時に、
 上記販売者端末は、
 クーボンの発券を要求した消費者端末から送信されてくるパスワードを受信し、受信したパスワードと、クーポンの効力に関するクーポン情報とを、自身だけしか暗号化できない暗号化方法で暗号化し、暗号化した結果である暗号化情報と、該クーポン情報とを、目視可能なデータとして記載したクーポンを作成し、作成したクーポンを消費者端末に対して送信し、
 クーボンの検証時に、
 上記販売者端末は、
 検証対象のクーポンが、上記消費者端末から送信されて使用が要求されたクーポンである場合には、
 該消費者端末から送信されてくるパスワードおよびクーポンを受信し、受信したパスワードおよびクーポン情報を、クーポンの発券時と同じ暗号化方法で暗号化し、暗号化した結果と、受信したクーポンに記載されている暗号化情報とが一致するか否かを検証し、
 検証対象のクーポンが、上記消費者端末で印刷されて使用が要求されたクーポンである場合には、
 印刷されたクーポンに記載されているクーポン情報および暗号化情報を取得し、消費者から提示されたパスワードおよび取得したクーポン情報を、クーポンの発券時と同じ暗号化方法で暗号化し、暗号化した結果と、取得した暗号化情報とが一致するか否かを検証することを特徴とする電子クーポン発券・検出方法。
 【請求項18】消費者が利用する少なくとも1つの消費者端末と、販売者が利用する少なくとも1つの販売者端末と、発券者が利用する少なくとも1つの発券者端末とが、ネットワークを介して相互に接続されてなるシステムにおいて、1枚で予め定めた効力を発揮するクーポンの発券および検証を行う方法であって、
 クーボンの発券時に、

上記発券者端末は、クーポンの発券を要求した消費者端末から送信されてくるパスワードを受信し、受信したパスワードと、クーポンの効力に関するクーポン情報とを、自身だけしか暗号化できない暗号化方法で暗号化し、暗号化した結果である暗号化情報と、該クーポン情報とを、目視可能なデータとして記載したクーポンを作成し、作成したクーポンを消費者端末に対して送信し、クーポンの検証時に、上記販売者端末は、検証対象のクーポンが、上記消費者端末から送信されて使用が要求されたクーポンである場合には、該消費者端末から送信されてくるパスワードおよびクーポンを受信し、受信したパスワードおよびクーポン情報を、上記発券者端末に対して送信して、該クーポンの検証を要求し、検証対象のクーポンが、上記消費者端末で印刷されて使用が要求されたクーポンである場合には、印刷されたクーポンを取得し、消費者から提示されたパスワードおよび取得したクーポンを、上記発券者端末に対して送信して、該クーポンの検証を要求し、上記発券者端末は、クーポンの検証を要求した販売者端末から送信されてくるパスワードおよびクーポンを受信し、受信したパスワードおよびクーポン情報を、クーポンの発券時と同じ暗号化方法で暗号化した結果と、受信したクーポンに記載されている暗号化情報とが一致するか否かを検証し、検証結果を該販売者端末に対して通知することを特徴とする電子クーポン発券・検出方法。

【発明の詳細な説明】

【0001】

【発明の属する技術分野】本発明は、インターネット等のネットワークを介して行われる電子商取引システムの利用環境において、各種商品やサービスと交換可能な電子クーポンを適正に取り扱うための電子クーポンシステムに関し、さらに詳しくは、ネットワークを介して電子クーポンを受け取った消費者が、該電子クーポンを、ネットワーク上に開設されたバーチャル販売店だけでなく、現実存在する販売店でも使用することができるようにした電子クーポンシステムに関する。

【0002】

【従来の技術】現在、商品券や割引券等といった、各種商品やサービスと交換できる券（以下、総じて「クーポン」と称す。）が普及している。この種のクーポンには、1枚で効力を発揮するものと、複数枚だけ集めたときに効力を発揮するものがあるが、効力が大きくなるほど、高度な印刷技術を用いることで偽造や改ざんを困難にするようにしたり、使用時に署名を確認することで第三者の不正使用を防止するようにしたりしている。

【0003】ところで、近年の情報機器の発達と通信環

境の整備により、インターネットのようなオープンなネットワークを介した電子商取引が盛んに行われるようになってきている。販売者は、ネットワーク上に仮想的な店舗を開設し、一般消費者に対して商品の販売を行う。

【0004】このようなネットワークを介した電子商取引においても、消費者サービスの一環としてクーポン（電子クーポン）を取り扱いたいという要求が高まっている。しかし、電子クーポンを単なる画像データとした場合は、正規手順で電子クーポンを受け取った消費者が、その電子クーポンをコピーして何度も使用したり、また、他の消費者に配布したりすることが簡単にできてしまう。さらに、オープンなネットワーク経由で電子クーポンを配布することから、第三者に盗聴され不正使用されてしまうという恐れもある。

【0005】このような不正行為を防止するための対策として、電子クーポンシステムにおいては、以下のような暗号技術が用いられている。

【0006】第1の対策として、電子クーポンシステムにおいては、電子クーポンの偽造や改ざんを防止するために、電子クーポンに販売者（発券元）のデジタル署名を付加し、使用時にそのデジタル署名を確認するようにしている。デジタル署名技術は、例えば、「暗号理論入門：岡本栄司著、共立出版（1996）」の133頁～138頁に開示されている。この文献での非対称暗号（公開鍵暗号）による署名方法を簡単に説明すると、以下のようである。

【0007】署名者は、署名したいメッセージ（または、メッセージのハッシュ値）を、署名者だけしか知らない秘密鍵を用いて暗号化することで、署名データを作成し、メッセージと署名データとをひとまとめにして検証者に渡す。検証者は、受け取った署名データを、上記秘密鍵に対応した公開鍵を用いて復号し、復号した結果と受け取ったメッセージとが一致していれば、上記署名者によって署名されたデータであると判断する。

【0008】また、第2の対策として、電子クーポンシステムにおいては、電子クーポンの二重使用を防止するために、各電子クーポンにシリアル番号を付加し、使用時にそのシリアル番号をチェックすることで、未使用の電子クーポンであるか否かを確認するようにしている。

【0009】さらに、第3の対策として、電子クーポンシステムにおいては、第三者による電子クーポンの不正使用を防止するために、メッセージを暗号化して送信するようにしている。メッセージを暗号化する方法としては、例えば、「OpenDesign（1996/6号 No.14）：CQ出版社」の101頁～112頁に記載されているSSL（Secure Socket Layer）等が挙げられる。

【0010】

【発明が解決しようとする課題】電子クーポンの発券から使用に至る全ての処理をネットワークを介して行うよ

うな電子クーポン専用のシステムの場合は、上述した全ての対策を講じるようにすることで、様々な不正行為を防止することができる。しかし、消費者の使い勝手を考慮すれば、消費者がネットワークを介して受け取った電子クーポンを紙に印刷し、従来の紙ベースのクーポンと同様に、販売店に持参して使用するような、紙クーポン・電子クーポン併用システムが好ましいが、そのようなシステムの場合には、電子クーポンに付加されたデジタル署名が印刷結果に反映されないことから、電子クーポンの偽造を防止することができない。

【0011】また、使用済みシリアル番号を販売店で管理しておくことで、クーポンの二重使用を防止することはできるが、ネットワークを介して受け取った電子クーポンが消費者端末の記憶装置から盗まれた場合や、印刷されたクーポンが盗まれた場合には、そのクーポンを第三者に不正使用されてしまうと、正当な消費者がクーポンを使用することができなくなってしまう。

【0012】さらに、複数枚だけ集めたときに効力を発揮するようなクーポン（以下、この種のクーポンを「チケット」と称す。）を取り扱う場合には、1枚で効力を発揮するクーポンに比べて発券枚数が多くなり、また、全ての消費者がチケットを集め終わるとは限らないので、消費者ごとに販売者側で管理するのは大変である。

【0013】本発明は、上記事情に鑑みてなされたものであり、その目的は、ネットワークを介して電子クーポンを受け取った消費者が、該電子クーポンを、ネットワーク上に開設されたバーチャル販売店だけでなく、現実存在する販売店でも使用することができるようにした電子クーポンシステムを提供することにある。

【0014】また、本発明の他の目的は、チケットを取り扱う場合に、販売者の手間を減らすことができるようにした電子クーポンシステムを提供することにある。

【0015】

【課題を解決するための手段】上記目的を達成するために、本発明は、第1の態様として、消費者が利用する少なくとも1つの消費者端末と、販売者が利用する少なくとも1つの販売者端末とが、ネットワークを介して相互に接続されてなり、上記消費者端末は、上記販売者端末に対して、消費者のパスワードを送信して、1枚で予め定めた効力を発揮するクーポンの発券を要求するクーポン発券要求手段と、上記販売者端末から送信されてくるクーポンを受信するクーポン受信手段と、上記販売者端末に対して、消費者のパスワードと、上記クーポン受信手段が受信したクーポンとを送信して、該クーポンの使用を要求するクーポン使用要求手段と、上記クーポン受信手段が受信したクーポンを印刷するクーポン印刷手段とを備え、上記販売者端末は、上記消費者端末から発券が要求されたクーポンを、該消費者端末に対して送信するクーポン発券手段と、上記消費者端末から送信されて使用が要求されたクーポン、および、上記消費者端末で

印刷されて使用が要求されたクーポンを検証するクーポン検証手段とを備え、上記販売者端末のクーポン発券手段は、上記消費者端末から送信されてきたパスワードを受信し、受信したパスワードの不可逆変換値と、クーポンの効力に関するクーポン情報と、該クーポン情報を、販売者だけしか知らない秘密の暗号鍵を用いて暗号化した暗号化情報とを、目視可能なデータとして記載したクーポンを作成し、作成したクーポンを該消費者端末に対して送信し、上記販売者端末のクーポン検証手段は、上記消費者端末から送信されて使用が要求されたクーポンを検証する場合に、該消費者端末から送信されてきたパスワードおよびクーポンを受信し、受信したパスワードの不可逆変換値と、受信したクーポンに記載されている不可逆変換値とが一致するか否かを検証すると共に、受信したクーポンに記載されているクーポン情報を、販売者だけしか知らない秘密の暗号鍵を用いて暗号化した暗号化情報と、受信したクーポンに記載されている暗号化情報とが一致するか否かを検証し、上記消費者端末で印刷されて使用が要求されたクーポンを検証する場合に、印刷されたクーポンに記載されている不可逆変換値とクーポン情報と暗号化情報とを取得し、消費者から提示されたパスワードの不可逆変換値と、取得した不可逆変換値とが一致するか否かを検証すると共に、取得したクーポン情報を、販売者だけしか知らない秘密の暗号鍵を用いて暗号化した暗号化情報と、取得した暗号化情報とが一致するか否かを検証することを特徴とした電子クーポンシステムを提供している。

【0016】第1の態様によれば、改ざんされては困るクーポン情報について、それを暗号化した暗号化情報を、目視可能なデータとして記載したクーポンを作成するようにしているので、消費者がクーポンを印刷して使用する場合でも、印刷されたクーポンに記載されている暗号化情報を検証することで、クーポンの偽造や改ざんを防止することができるようになる。

【0017】また、第1の態様によれば、クーポンの発券時に消費者が提示したパスワードについて、その不可逆変換値を、目視可能なデータとして記載したクーポンを作成するようにしているので、クーポンの使用時に消費者が提示したパスワードの不可逆変換値と、クーポンに記載されている不可逆変換値とを比較することで、第三者によるクーポンの不正使用を検出することができるようになる。

【0018】なお、第1の態様において、上記販売者端末のクーポン発券手段は、上述した動作ではなく、上記消費者端末から送信されてきたパスワードを受信し、受信したパスワードの不可逆変換値と、クーポンの効力に関するクーポン情報とを連結し、連結した結果を、公開鍵暗号方式における販売者の秘密鍵を用いて暗号化したデジタル署名と、上記クーポン情報とを、目視可能なデータとして記載したクーポンを作成し、作成したクーポン

ンを該消費者端末に対して送信するようにしてもよく、このようにした場合は、上記販売者端末のクーポン検証手段は、上記消費者端末から送信されて使用が要求されたクーポンを検証する場合に、該消費者端末から送信されてきたパスワードおよびクーポンを受信し、受信したクーポンに記載されているデジタル署名を、公開鍵暗号方式における販売者の公開鍵を用いて復号した結果得られるパスワードの不可逆変換値と、受信したパスワードの不可逆変換値とが一致するか否かを検証すると共に、受信したクーポンに記載されているデジタル署名を、公開鍵暗号方式における販売者の公開鍵を用いて復号した結果得られるクーポン情報と、受信したクーポンに記載されているクーポン情報とが一致するか否かを検証し、上記消費者端末で印刷されて使用が要求されたクーポンを検証する場合に、印刷されたクーポンに記載されているクーポン情報とデジタル署名とを取得し、取得したデジタル署名を、公開鍵暗号方式における販売者の公開鍵を用いて復号した結果得られるパスワードの不可逆変換値と、消費者から提示されたパスワードの不可逆変換値とが一致するか否かを検証すると共に、取得したデジタル署名を、公開鍵暗号方式における販売者の公開鍵を用いて復号した結果得られるクーポン情報と、取得したクーポン情報とが一致するか否かを検証するようにすることができる。

【0019】さらに、第1の態様において、上記販売者端末のクーポン発券手段は、作成したクーポンと共に、公開鍵暗号方式における販売者の秘密鍵を用いて該クーポン全体を暗号化したデジタル署名を、上記消費者端末に対して送信するようにし、上記消費者端末のクーポン受信手段は、受信したクーポンと、該クーポンと共に送信されてきたデジタル署名を、公開鍵暗号方式における販売者の公開鍵を用いて復号した結果とが一致するか否かを検証するようにしてもよい。

【0020】このようにすれば、クーポンの使用時だけではなく、クーポンの発券時に、クーポンの発券を受けた消費者側で、受け取ったクーポンを検証することができるようになる。

【0021】さらに、第1の態様において、上記クーポン情報が、クーポンごとに固有のシリアル番号を含むようにし、上記販売者端末は、効力を発揮済みのクーポンに記載されているクーポン情報中のシリアル番号を記憶するシリアル番号記憶手段を備えるようにし、上記販売者端末のクーポン検証手段は、検証対象のクーポンに記載されているクーポン情報中のシリアル番号を、上記シリアル番号記憶手段が記憶済みでないか否かを検証するようにしてもよい。

【0022】このようにすれば、クーポンの偽造や改ざん、および、第三者によるクーポンの不正使用に加えて、クーポンの二重使用も防止することができるようになる。

【0023】また、上記他の目的を達成するために、本発明は、第2の態様として、第1の態様において、上記消費者端末は、上記販売者端末に対して、消費者のパスワードを送信して、予め定めた n ($n > 1$)枚だけ集めたときに予め定めた効力を発揮するクーポン（以下、「チケット」と称す。）のうちの、1枚目のチケットの発券を要求する初期チケット発券要求手段と、上記販売者端末に対して、消費者のパスワードと、発券済みのチケットのうちの最新のチケット（以下、「発券済み最新チケット」と称す。）とを送信して、2枚目以降のチケットの発券を要求するチケット発券要求手段と、上記販売者端末から送信されてくるチケットを受信して保存するチケット受信手段とを備え、上記販売者端末は、上記消費者端末から発券が要求された1枚目のチケットを、該消費者端末に対して送信する初期チケット発券手段と、上記消費者端末から発券が要求された2枚目以降のチケットを、該消費者端末に対して送信するチケット発券手段とを備え、上記販売者端末の初期チケット発券手段は、上記消費者端末から送信されてきたパスワードを受信し、受信したパスワードと、 n 枚のチケットの組を識別するために付与した固有の値（以下、「UID」と称す。）と、販売者だけしか知らない秘密の情報とを連結し、連結した結果の不可逆変換値 H_1 に基づいて、不可逆変換値 H_i ($1 \leq i < n$)の不可逆変換値 H_{i+1} を順次計算し、上記UIDおよび不可逆変換値 H_n を、1枚目のチケットとして、該消費者端末に対して送信し、上記販売者端末のチケット発券手段は、上記消費者端末から送信されてきたパスワードおよび発券済み最新チケットを受信し、受信したパスワードと、受信した発券済み最新チケットのうちのUIDと、販売者だけしか知らない秘密の情報とを連結し、連結した結果の不可逆変換値 H_1 に基づいて、不可逆変換値 H_i ($1 \leq i < n$)の不可逆変換値 H_{i+1} を順次計算し、受信した発券済み最新チケットのうちの不可逆変換値 H_m ($1 \leq m \leq n$)と、不可逆変換値 H_1 とが一致したならば、 n 枚のチケットの発券を完了し、一致しないならば、上記UIDおよび不可逆変換値 H_{n-1} を、次のチケットとして、該消費者端末に対して送信することを特徴とした電子クーポンシステムを提供している。

【0024】第2の態様によれば、消費者だけしか知らない情報であるパスワードと、販売者だけしか知らない秘密の情報（例えば、公開鍵暗号方式における販売者の秘密鍵）と、 n 枚のチケットの組を識別するためのUIDとを連結したものから、不可逆変換値を繰り返して計算し、 n 番目の計算結果、 $n-1$ 番目の計算結果、…、2番目の計算結果、1番目の計算結果という順番で、各計算結果をチケットとして発券するようにしているので、販売店側で、消費者ごとに既に何枚のチケットを発券したかを管理する必要がなくなる。

【0025】なお、第2の態様において、上記販売者端

末の初期チケット発券手段は、上述した動作ではなく、上記消費者端末から送信されてきたパスワードを受信し、受信したパスワードと、 n 枚のチケットの組を識別するために付与した固有の値（以下、「UID」と称す。）とを連結し、販売者だけしか知らない秘密の暗号鍵を用いて、連結した結果を暗号化した暗号化情報 H_1 を計算すると共に、計算した暗号化情報 H_1 に基づいて、暗号化情報 H_i ($1 \leq i < n$) の暗号化情報 H_{i+1} を順次計算し、上記UIDおよび暗号化情報 H_n を、1枚目のチケットとして、該消費者端末に対して送信するようにし、上記販売者端末のチケット発券手段は、上述した動作ではなく、上記消費者端末から送信されてきたパスワードおよび発券済み最新チケットを受信し、受信したパスワードと、受信した発券済み最新チケットのうちのUIDとを連結し、販売者だけしか知らない秘密の暗号鍵を用いて、連結した結果を暗号化した暗号化情報 H_1 を計算すると共に、計算した暗号化情報 H_1 に基づいて、暗号化情報 H_i ($1 \leq i < n$) の暗号化情報 H_{i+1} を順次計算し、受信した発券済み最新チケットのうちの暗号化情報 H_m ($1 \leq m \leq n$) と、暗号化情報 H_1 とが一致したならば、 n 枚のチケットの発券を完了し、一致しないならば、上記UIDおよび暗号化情報 H_{n-1} を、次のチケットとして、該消費者端末に対して送信するようにしてもよい。

【0026】また、第2の態様において、上記販売者端末の初期チケット発券手段は、上述した動作ではなく、上記販売者端末の初期チケット発券手段は、上記消費者端末から送信されてきたパスワードを受信し、受信したパスワードと、 n 枚のチケットの組を識別するために付与した固有の値（以下、「UID」と称す。）と、1枚目のチケットである旨を示す枚数情報とを連結し、販売者だけしか知らない秘密の暗号鍵を用いて、連結した結果を暗号化した暗号化情報 H_1 を、1枚目のチケットとして、該消費者端末に対して送信するようにし、上記販売者端末のチケット発券手段は、上述した動作ではなく、上記消費者端末から送信されてきたパスワードおよび発券済み最新チケットを受信し、受信した発券済み最新チケットである暗号化情報 H_m ($1 \leq m \leq n$) を、販売者だけしか知らない秘密の暗号鍵を用いて復号した結果得られる枚数情報が、 n 枚目のチケットである旨を示す枚数情報であるならば、 n 枚のチケットの発券を完了し、そうでないならば、受信したパスワードと、受信した発券済み最新チケットである暗号化情報 H_m ($1 \leq m \leq n$) を、販売者だけしか知らない秘密の暗号鍵を用いて復号した結果得られるUIDと、 $m+1$ 枚目のチケットである旨を示す枚数情報とを連結し、販売者だけしか知らない秘密の暗号鍵を用いて、連結した結果を暗号化した暗号化情報 H_{m+1} を、次のチケットとして、該消費者端末に対して送信するようにしてもよい。

【0027】

【発明の実施の形態】以下、本発明の実施の形態について図面を参照して説明する。

【0028】なお、以下の説明で参照する図面において、同一の符号は、同様の構成要素を表すものとする。また、これにより本発明が限定されるものではない。

【0029】（第1の実施形態）まず、本発明の第1の実施形態について説明する。

【0030】図1は、第1の実施形態に係る電子クーポンシステムの概略構成を示す図である。

【0031】第1の実施形態に係る電子クーポンシステムは、消費者200₁～200_n（以下、単に「消費者200」とも称す。）および販売者100が利用するシステムであり、図1に示すように、消費者200が利用する端末である消費者端末201₁～201_n（以下、単に「消費者端末201」とも称す。）と、販売者100が利用する端末である販売者端末101とが、インターネット等の通信網300を介して互いに接続されて構成されている。

【0032】第1の実施形態に係る電子クーポンシステムにおいては、消費者200が、消費者端末201を利用して、通信網300を介して販売者端末101との間でデータをやり取りすることで、販売者100に対してクーポンの発券を要求したり、販売者100によって発券されたクーポンの使用を要求したりすることができるようにしている。このとき、販売者100は、販売者端末101を利用して、消費者200に対してクーポンを発券したり、消費者200によって使用されるクーポンを検証したりする。

【0033】特に、第1の実施形態に係る電子クーポンシステムにおいては、消費者200が、消費者端末201を利用して、販売者100によって発券されたクーポンを印刷し、印刷したクーポンを販売店に持参することで、直接、販売者100に対してクーポンの使用を要求することもできるようにしている。このとき、販売者100は、販売者端末101を利用して、消費者200が持参したクーポンを検証する。

【0034】すなわち、第1の実施形態に係る電子クーポンシステムは、通信網300を介して行われる電子商取引環境を実現すると共に、消費者200が、販売者100によって発券されたクーポンを、通信網300上に開設されたバーチャル販売店だけではなく、現実存在する販売店でも使用することができるようにしたものである。

【0035】次に、第1の実施形態に係る電子クーポンシステムを構成する販売者端末101および消費者端末201のハードウェア構成について、図2および図3を用いて説明する。

【0036】図2は販売者端末101のハードウェア構成を示す図である。

【0037】図2に示すように、販売者端末101は、

通信インタフェース102と、表示装置103と、入力装置104と、記憶装置105と、中央処理装置(CPU)106と、一時記憶装置(メモリ)107とが、バス110によって互いに接続された構成となっている。

【0038】通信インタフェース102は、通信網300を介して、消費者端末201との間でデータのやり取りを行うためのインタフェースである。

【0039】また、表示装置103は、販売者端末101を利用する販売者100に対するメッセージ等を表示するために用いられるものであり、CRTや液晶ディスプレイ等で構成される。

【0040】また、入力装置104は、販売者端末101を利用する販売者100がデータや命令等を入力するために用いられるものであり、キーボードやマウス等で構成される。

【0041】また、記憶装置105は、販売者端末101で使用されるプログラムやデータを永続的に記憶するために用いられるものであり、ハードディスクやフロッピーディスク等で構成される。

【0042】また、CPU106は、販売者端末101の構成要素を統括的に制御したり、様々な演算処理を行ったりする。

【0043】また、メモリ107には、オペレーティングシステム(以下、「OS」と称す。)107aや、クーポン発券・検証処理プログラム107bといった、CPU106が実行するプログラム等が一時的に格納される。

【0044】ここで、OS107aは、販売者端末101全体の制御を行うために、ファイル管理、プロセス管理、デバイス管理といった機能を実現するためのプログラムである。また、クーポン発券・検証処理プログラム107bは、消費者200に対してクーポンを発券したり、消費者200から使用が要求されたクーポンを検証したりするためのプログラムである。

【0045】図3は消費者端末201のハードウェア構成を示す図である。

【0046】図3に示すように、消費者端末201は、通信インタフェース202と、表示装置203と、入力装置204と、記憶装置205と、中央処理装置(CPU)206と、一時記憶装置(メモリ)207と、印刷装置208とが、バス210によって互いに接続された構成となっている。

【0047】通信インタフェース202は、通信網300を介して、販売者端末101との間でデータのやり取りを行うためのインタフェースである。

【0048】また、表示装置203は、消費者端末201を利用する消費者200に対するメッセージ等を表示するために用いられるものであり、CRTや液晶ディスプレイ等で構成される。

【0049】また、入力装置204は、消費者端末20

1を利用する消費者200がデータや命令等を入力するために用いられるものであり、キーボードやマウス等で構成される。

【0050】また、記憶装置205は、消費者端末201で使用されるプログラムやデータを永続的に記憶するために用いられるものであり、ハードディスクやフロッピーディスク等で構成される。

【0051】また、CPU206は、消費者端末201の構成要素を統括的に制御したり、様々な演算処理を行ったりする。

【0052】また、メモリ207には、OS207aや、クーポン要求・受信・発信処理プログラム207bといった、CPU206が実行するプログラム等が一時的に格納される。

【0053】ここで、OS207aは、消費者端末201全体の制御を行うために、ファイル管理、プロセス管理、デバイス管理といった機能を実現するためのプログラムである。また、クーポン要求・受信・発信処理プログラム207bは、販売者100に対してクーポンの発券を要求したり、販売者100によって発券されたクーポンを受信したり、販売者100に対してクーポンの使用を要求したりするためのプログラムである。

【0054】また、印刷装置208は、電子的なデータを印刷するために用いられるものであり、プリンタ等で構成される。

【0055】次に、第1の実施形態に係る電子クーポンシステムの動作について説明する。

【0056】なお、以下の説明において、消費者200が行う処理は、実際には、消費者200の指示によって消費者端末201が実行し、販売者100が行う処理は、実際には、販売者100の指示によって販売者端末101が実行するものである。

【0057】図4は、消費者200が、販売者100に対してクーポンの発券を要求し、販売者100によって発券されたクーポンを受信するまでの動作を説明するための図である。

【0058】図4において、まず、消費者200は、販売者100からクーポンの発券を受ける条件を満たしているものとする(S2000)。

【0059】消費者200は、後述するクーポン要求処理(S2400)を行い、暗号化した自身のパスワード501を、販売者100に対して送信する。

【0060】販売者100は、パスワード501を受信すると、後述するクーポン発券処理(S1300)を行い、クーポン502と、クーポン502のデジタル署名503とを、消費者200に対して送信する。

【0061】消費者200は、クーポン502およびデジタル署名503を受信すると、後述するクーポン受信処理(S2500)を行い、受信したクーポン502を保管する。

【0062】図5は、既にクーポンの発券を受けている消費者200が、通信網300を介してクーポンを使用し、販売者100が、クーポンを検証するまでの動作を説明するための図である。

【0063】図5において、既にクーポンの発券を受けている消費者200は、後述するクーポン使用オンライン処理(S2600)を行い、クーポン受信処理(S2500)で入手したクーポン502と、暗号化した自身のパスワード501とを、販売者100に対して送信する。

【0064】販売者100は、クーポン502およびパスワード501を受信すると、後述するクーポン検証処理(S1400)を行い、受信したクーポン502を検証する。

【0065】図6は、既にクーポンの発券を受けている消費者200が、クーポンを印刷し、印刷されたクーポンを販売店に持参して使用し、販売者100が、クーポンを検証するまでの動作を説明するための図である。

【0066】図6において、既にクーポンの発券を受けている消費者200は、後述するクーポン使用オフライン処理(S2700)を行い、印刷されたクーポン504を販売店に持参する。

【0067】販売者100は、消費者200が持参したクーポン504を受け取ると、クーポン検証処理(S1400)を行い、受け取ったクーポン504を検証する。

【0068】図7は、図4のクーポン要求処理(S2400)の処理フローチャートであり、本処理は、クーポン要求・受信・発信処理プログラム207bによって実現される。

【0069】図7に示すように、クーポン要求処理(S2400)において、消費者200は、まず、販売者100に対して、公開鍵暗号方式における販売者100の公開鍵を要求し、公開鍵を受信する(ステップ2401)。

【0070】続いて、消費者200は、自身だけしか知らないパスワードを入力する(ステップ2402)。

【0071】続いて、消費者200は、ステップ2402で入力したパスワードを、ステップ2401で入手した公開鍵を用いて暗号化し(ステップ2403)、暗号化したパスワード501を、販売者100に対して送信する(ステップ2404)。

【0072】図8は、図4のクーポン発券処理(S1300)の処理フローチャートであり、本処理は、クーポン発券・検証処理プログラム107bによって実現される。

【0073】図8に示すように、クーポン発券処理(S1300)において、販売者100は、まず、暗号化されたパスワード501を受信すると(ステップ1301)、受信したパスワード501を、公開鍵暗号方式に

おける販売者100の秘密鍵を用いて復号する(ステップ1302)。ここでは、公開鍵暗号技術を使ってパスワードを暗号化する例を示しているが、パスワードが通信網300を通過する際に盗聴されなければ、どのような暗号技術を使ってもかまわない。

【0074】続いて、販売者100は、ステップ1302で復号したパスワード501に不可逆変換を施す(ステップ1303)。以下、パスワードに不可逆変換を施した結果を、パスワードの不可逆変換値またはPHと称す。

【0075】続いて、販売者100は、シリアル番号、有効期限、クーポンの価値(例えば、金額)等の、クーポンの効力に関するクーポン情報を設定し(ステップ1304)、設定したクーポン情報のデジタル署名を、販売者100の秘密鍵を用いて計算する(ステップ1305)。そして、ステップ1303で計算した不可逆変換値、ステップ1304で設定したクーポン情報、ステップ1305で計算したデジタル署名を、目視可能なデータ(例えば、数字や文字等)として記載したクーポンを作成することで、書面としてのクーポン502を作成する(ステップ1306)。

【0076】続いて、販売者100は、書面としてのクーポン502全体のデジタル署名503を、販売者100の秘密鍵を用いて計算し(ステップ1307)、ステップ1306で作成したクーポン502と、ステップ1307で計算したデジタル署名503とを、消費者200に対して送信する(ステップ1308)。

【0077】図9は、図4のクーポン受信処理(S2500)の処理フローチャートであり、本処理は、クーポン要求・受信・発信処理プログラム207bによって実現される。

【0078】図9に示すように、クーポン受信処理(S2500)において、消費者200は、販売者100が送信したクーポン502およびデジタル署名503を受信すると(ステップ2501)、受信したデジタル署名503を検証することで、受信したクーポン502が、通信網300を介して送信されてくる間に改ざんされていないか否かを検証する(ステップ2502)。ステップ2502では、詳しくは、消費者200は、受信したクーポン502と、受信したデジタル署名503を販売者100の公開鍵を用いて復号した結果とを比較し、両者が一致すれば、受信したクーポン502が改ざんされていないと判断する。

【0079】そして、改ざんされていないならば、受信したクーポン502を記憶装置205に保存する(ステップ2503)。

【0080】ここで、クーポン502は、例えば、図14に示すような形式とすることができ、受信時に表示装置203に表示されるようにすることが好ましい。

【0081】図10は、図5のクーポン使用オンライン

処理（S2600）の処理フローチャートであり、本処理は、クーポン要求・受信・発信処理プログラム207bによって実現される。

【0082】図10に示すように、クーポン使用オンライン処理（S2600）において、消費者200は、まず、販売者100に対して、販売者100の公開鍵を要求し、公開鍵を受信する（ステップ2601）。

【0083】続いて、消費者200は、自身だけしか知らないパスワード（クーポン要求処理（S2400）で入力したパスワードと同一のパスワード）を入力する（ステップ2602）。

【0084】続いて、消費者200は、ステップ2602で入力したパスワードを、ステップ2601で入手した公開鍵を用いて暗号化し（ステップ2603）、暗号化したパスワード501と、図9に示したクーポン受信処理（S2500）で入手したクーポン502とを、販売者100に対して送信する（ステップ2604）。

【0085】図11は、図6のクーポン使用オフライン処理（S2700）の処理フローチャートであり、本処理は、クーポン要求・受信・発信処理プログラム207bによって実現される。

【0086】図11に示すように、クーポン使用オフライン処理（S2700）において、消費者200は、図9に示したクーポン受信処理（S2500）で入手したクーポン502を、印刷装置208で印刷する（ステップ2701）。

【0087】ここで、印刷されたクーポン504の形式は、図14に示したクーポン502の形式と同様の形式である。

【0088】続いて、消費者200は、印刷されたクーポン504を販売店に持参し、自身だけしか知らないパスワード（クーポン要求処理（S2400）で入力したパスワードと同一のパスワード）を、販売者100に告げる（ステップ2702）。なお、ステップ2702は、消費者200自身が行う行動であり、消費者端末201では実行されない。

【0089】図12は、図5および図6のクーポン検証処理（S1400）の処理フローチャートであり、本処理は、クーポン発券・検証処理プログラム107bによって実現される。

【0090】図12に示すように、クーポン検証処理（S1400）は、使用されるクーポンが、通信網300を介してオンラインで届いたクーポン502であるか、または、直接持参されたクーポン（印刷されたクーポン）504であるかによって、処理が分かれる（ステップ1401）。

【0091】直接持参されたクーポン504である場合には、販売者100は、ステップ1404の書面検証処理から処理を開始する。ただし、このとき、販売者100は、クーポン504に記載されている各種情報を取得

する必要があるが、取得方法については任意である。

【0092】また、通信網300を介してオンラインで届いたクーポン502である場合には、販売者100は、このクーポン502と共に、暗号化されたパスワード501を受信し（ステップ1402）、受信したパスワード501を、販売者100の秘密鍵を用いて復号する（ステップ1403）。

【0093】ステップ1404では、販売者100は、クーポンに記載されている各種情報を検証する書面検証処理を行う。なお、書面検証処理の詳細については後述する。

【0094】ステップ1404の書面検証処理の結果、全ての情報についての検証に合格した場合には（ステップ1405）、クーポンの二重使用を防止するために、クーポンに記載されているクーポン情報中のシリアル番号を、使用済みシリアル番号リストに登録し（ステップ1406）、クーポンの定められた効力を発揮させる（ステップ1407）。また、1つでも不合格であった場合には（ステップ1405）、エラー処理を実行する（ステップ1408）。

【0095】図13は、図12の書面検証処理（ステップ1404）の処理フローチャートである。

【0096】図13に示すように、書面検証処理（ステップ1404）において、販売者100は、まず、書面としてのクーポンに記載されているクーポン情報のデジタル署名を、販売者100の秘密鍵を用いて計算する（ステップ1410）。

【0097】そして、検証に合格しなければ（ステップ1411）、すなわち、計算したデジタル署名と、クーポンに記載されているデジタル署名とが一致しなければ、クーポンが改ざんされているので、エラー処理を実行する（ステップ1417）。

【0098】また、検証に合格すれば（ステップ1411）、すなわち、計算したデジタル署名と、クーポンに記載されているデジタル署名とが一致すれば、ステップ1403で得たパスワード（または、消費者200から告げられたパスワード）の不可逆変換値を計算し、計算した不可逆変換値と、書面としてのクーポンに記載されている不可逆変換値と比較する（ステップ1412）。

【0099】ステップ1412の比較の結果、両者が一致しなければ（ステップ1413）、クーポン発券時のパスワードを知らない第三者によるクーポンの不正使用であると考えられるので、エラー処理を実行する（ステップ1418）。

【0100】また、販売者100は、書面としてのクーポンに記載されているクーポン情報中のシリアル番号が、使用済みシリアル番号リストに登録されているか否かを検証する（ステップ1414）。既に登録されているならば（ステップ1415）、クーポンの二重使用という理由で、エラー処理を実行する（ステップ141

9)。

【0101】最後に、販売者100は、書面としてのクーポンに記載されているクーポン情報中の有効期限を参照し、有効期限内のクーポンであるか否かを検証し(ステップ1416)、有効期限外であれば、有効期限切れのエラー処理を実行する(ステップ1420)。

【0102】これら全ての検証に合格すれば、クーポンは有効となり、効力が発揮されることとなる。

【0103】以上説明したように、第1の実施形態に係る電子クーポンシステムにおいては、シリアル番号、有効期限、金額等の改ざんされては困るクーポン情報のデジタル署名を、販売者100だけしか知らない情報である秘密鍵を用いて計算し、計算したデジタル署名を、目視可能なデータとして記載したクーポンを作成するようにしている。

【0104】従って、第1の実施形態に係る電子クーポンシステムによれば、消費者200が電子的なクーポンを印刷して使用する場合でも、印刷されたクーポンに記載されているデジタル署名を検証することで、クーポンの偽造や改ざんを検出することができる。

【0105】また、第1の実施形態に係る電子クーポンシステムにおいては、クーポンの発券時に、消費者200が提示したパスワードの不可逆変換値を、目視可能なデータとして記載したクーポンを作成するようにしている。さらに、クーポンの使用時には、発券を要求した消費者200だけしか知らないパスワードを販売者100に提示し、消費者200が提示したパスワードの不可逆変換値と、クーポンに記載されている不可逆変換値とを比較するようにしている。

【0106】従って、第1の実施形態に係る電子クーポンシステムによれば、たとえクーポンが盗まれたとしても、クーポンの発券要求時に提示されたパスワードを知らない第三者がクーポンを不正使用するのを防止することができる。

【0107】なお、第1の実施形態に係る電子クーポンシステムにおいては、クーポン情報について、公開鍵暗号方式における販売者100の秘密鍵を用いて計算したデジタル署名を、目視可能なデータとしてクーポンに記載するようにした例を示しているが、販売者100だけしか知らない秘密の暗号鍵を用いて暗号化した暗号化情報を、目視可能なデータとしてクーポンに記載するようにし、この暗号化情報を検証するようにしてもよい。

【0108】また、第1の実施形態に係る電子クーポンシステムにおいては、パスワードについて、不可逆変換を施した不可逆変換値を、目視可能なデータとしてクーポンに記載するようにした例を示しており、本例によれば、不可逆変換方法を公開しても支障がないので、パスワードの不可逆変換値が不一致である場合に、消費者200が、自身が提示したパスワードの不可逆変換値を計算して確認することが可能である。しかしながら、パス

ワードについて、販売者100だけしか暗号化できない暗号化方法で暗号化した暗号化情報を、目視可能なデータとしてクーポンに記載するようにし、この暗号化情報を検証するようにしてもよい。

【0109】なお、本発明は、上述した第1の実施形態に限定されるものではなく、その要旨の範囲内で様々な変形が可能である。

【0110】例えば、第1の実施形態に係る電子クーポンシステムにおいては、消費者200は、販売者100に対してパスワードを送信するときに、販売者100の公開鍵を取得し、暗号通信を行うようにしているが、本発明はこれに限定しない。消費者200は、1度、販売者100の公開鍵を入手すれば、2回以降は、その公開鍵を使うことができる。また、販売者100と消費者200との間で共通の鍵を持つことができれば、秘密鍵暗号技術を使って暗号化するようにしてもよい。

【0111】また、第1の実施形態に係る電子クーポンシステムにおいて、消費者200から販売者100に対してパスワードを送信するときに、暗号化されたパスワードがそのまま盗まれて不正使用されるのを防止するために、パスワードを、その他の情報(乱数や適当な数字でよい。)と共に暗号化して送信するようにしてもよい。

【0112】また、第1の実施形態に係る電子クーポンシステムにおいては、販売者100は、デジタル署名を、数値や文字等の目視可能なデータとしてクーポンに記載するようにしているが、印刷後に目視可能であれば、例えば、バーコード等のようなものであってもよい。バーコードとして記載すれば、販売者100は、印刷されたクーポンから各種情報を取得する際に、バーコードリーダを用いることができるようになる。

【0113】また、第1の実施形態に係る電子クーポンシステムにおいては、販売者100は、消費者200のパスワードの不可逆変換値と、シリアル番号、有効期限、金額等のクーポン情報のデジタル署名とを、別々にクーポンに記載するようにしているが、クーポン情報と共に、パスワードも一緒にデジタル署名を計算するようにしてもよい。また、このとき、クーポン情報やパスワード等の、デジタル署名を計算する元の情報は、不可逆変換を施した後に、デジタル署名を計算するようにしてもよい。

【0114】(第2の実施形態)ところで、クーポンは、販売者100の販売方針により、1枚で効力を発揮するものと、ある種の条件を満たしたときのみ、効力を発揮するものがある。例えば、予め定めた枚数だけ集めたときに効力を発揮するようなクーポン(以下、この種のクーポンを、特に「チケット」と称す。)を取り扱うようにした場合を、第2の実施形態として、上述した第1の実施形態と異なる点についてのみ説明する。

【0115】第2の実施形態に係る電子クーポンシステム

ムの概略構成は、図1に示した概略構成と同様である。

【0116】図15は販売者端末101のハードウェア構成を示す図である。

【0117】図2に示したハードウェア構成と異なる点は、メモリ107に、チケット発券・検証処理プログラム107cが一時的に格納される点である。

【0118】チケット発券・検証処理プログラム107cは、消費者200に対してチケットを発券したり、消費者200から使用が要求されたチケットを検証したりするためのプログラムである。

【0119】図16は消費者端末201のハードウェア構成を示す図である。

【0120】図3に示したハードウェア構成と異なる点は、メモリ207に、チケット要求・受信・発信処理プログラム207cが一時的に格納される点である。

【0121】チケット要求・受信・発信処理プログラム207cは、販売者100に対してチケットの発券を要求したり、販売者100によって発券されたチケットを受信したり、販売者100に対してチケットの使用を要求したりするためのプログラムである。

【0122】次に、第2の実施形態に係る電子クーポンシステムの動作について説明する。

【0123】なお、以下の説明においても、上述した第1の実施形態と同様に、消費者200が行う処理は、実際には、消費者200の指示によって消費者端末201が実行し、販売者100が行う処理は、実際には、販売者100の指示によって販売者端末101が実行するものである。

【0124】図17は、消費者200が、販売者100に対して1枚目のチケットの発券を要求し、販売者100によって発券された1枚目のチケットを受信するまでの動作を説明するための図である。なお、チケットは、n枚だけ集めたときに効力を発揮するものとする。

【0125】図17において、まず、消費者200は、後述する初期チケット発券要求処理(S2100)を行い、暗号化した自身のパスワード501を、販売者100に対して送信する。

【0126】販売者100は、パスワード501を受信すると、後述する初期チケット発券処理(S1100)を行い、n枚のチケットの組を識別するために付与した固有の値(以下、「UID」と称す。)505と、受信したパスワード501、UID505、販売者100だけしか知らない秘密の情報(例えば、販売者100の秘密鍵)を連結したものの、n番目の不可逆変換値 $H_n(506_n)$ とを、1枚目のチケットとして、消費者200に対して送信する。

【0127】消費者200は、UID505および $H_n(506_n)$ を受信すると、後述するチケット受信処理(S2200)を行い、受信したUID505および $H_n(506_n)$ を保管する。

【0128】図18は、消費者200が、販売者100に対して2枚目以降のチケットの発券を要求し、販売者100によって発券された2枚目以降のチケットを受信するまでの動作を説明するための図である。

【0129】図18において、まず、消費者200は、2枚目のチケットの発券を受ける場合は、後述するチケット発券要求処理(S2300)を行い、暗号化した自身のパスワード501と、1枚目のチケット受信処理(S2200)で入手したUID505および $H_n(506_n)$ とを、販売者100に対して送信する。

【0130】販売者100は、パスワード501、UID505、 $H_n(506_n)$ を受信すると、後述するチケット発券処理(S1200)を行い、受信したパスワード501、UID505、 $H_n(506_n)$ と、販売者100の秘密鍵とから、 $H_{n-1}(506_{n-1})$ を求めて、求めた $H_{n-1}(506_{n-1})$ を、2枚目のチケットとして、消費者200に対して送信する。

【0131】消費者200は、 $H_{n-1}(506_{n-1})$ を受信すると、チケット受信処理(S2200)を行い、受信した $H_{n-1}(506_{n-1})$ を保管する。

【0132】同様に、消費者200は、 $m+1$ 枚目($1 \leq m < n$)のチケットの発券を受ける場合は、チケット発券要求処理(S2300)を行い、暗号化した自身のパスワード501と、 m 枚目のチケット受信処理(S2200)で入手したUID505および $H_{n-(m-1)}(506_{n-(m-1)})$ とを、販売者100に対して送信する。

【0133】販売者100は、パスワード501、UID505、 $H_{n-(m-1)}(506_{n-(m-1)})$ を受信すると、チケット発券処理(S1200)を行い、受信したパスワード501、UID505、 $H_{n-(m-1)}(506_{n-(m-1)})$ と、販売者100の秘密鍵とから、 $H_{n-m}(506_{n-m})$ を求めて、求めた $H_{n-m}(506_{n-m})$ を、 $m+1$ 枚目のチケットとして、消費者200に対して送信する。

【0134】消費者200は、 $H_{n-m}(506_{n-m})$ を受信すると、チケット受信処理(S2200)を行い、受信した $H_{n-m}(506_{n-m})$ を保管する。

【0135】このようにして、消費者200は、n枚のチケットを集めることができ、これらn枚のチケットの効力を発揮させたい場合には、チケット発券要求処理(S2300)を行い、暗号化された自身のパスワード501と、n枚目のチケット受信処理(S2200)で入手したUID505および $H_1(506_1)$ とを、販売者100に対して送信する。

【0136】販売者100は、パスワード501、UID505、 $H_1(506_1)$ を受信すると、チケット発券処理(S1200)を行い、受信したパスワード501、UID505、 $H_1(506_1)$ と、販売者100の秘密鍵とから、消費者200がn枚だけチケットを集めたことを確認し、n枚のチケット収集終了処理(S1250)を行う。

【0137】図19は、図17の初期チケット発券要求処理(S2100)の処理フローチャートであり、本処理は、チケット要求・受信・発信処理プログラム207cによって実現される。

【0138】図19に示すように、初期チケット発券要求処理(S2100)において、消費者200は、まず、販売者100に対して、販売者100の公開鍵を要求し、公開鍵を受信する(ステップ2101)。

【0139】続いて、消費者200は、自身だけしか知らないパスワードを入力する(ステップ2102)。

【0140】続いて、消費者200は、ステップ2102で入力したパスワードを、ステップ2101で入手した公開鍵を用いて暗号化し(ステップ2103)、暗号化したパスワード501を、販売者100に対して送信する(ステップ2104)。

【0141】図20は、図17の初期チケット発券処理(S1100)の処理フローチャートであり、本処理は、チケット発券・検証処理プログラム107cによって実現される。

【0142】図20に示すように、初期チケット発券処理(S1100)において、販売者100は、まず、暗号化されたパスワード501を受信すると(ステップ1101)、受信したパスワード501を、販売者100の秘密鍵を用いて復号する(ステップ1102)。ここでは、公開鍵暗号技術を使ってパスワードを暗号化する例を示しているが、パスワードが通信網300を通過する際に盗聴されなければ、どのような暗号技術を使ってもかまわない。

【0143】続いて、販売者100は、 n 枚のチケットの組を識別するための固有の値であるUID505を作成し(ステップ1103)、ステップ1102で復号したパスワード、ステップ1103で作成したUID505、販売者100の秘密鍵を結合したものに、不可逆変換を施す(ステップ1104)。以下、パスワード、UID、秘密鍵を結合したものに不可逆変換を施した結果を、不可逆変換値 H_m ($1 \leq m \leq n$)と称すが、ステップ1104で計算される不可逆変換値 H_m は H_1 (506₁)である。

【0144】続いて、販売者100は、 H_i の不可逆変換値 H_{i+1} ($1 \leq i < n$)を計算する(ステップ1105)。ステップ1105では、詳しくは、販売者100は、図24に示すように、まず、 H_1 (506₁)の不可逆変換値 H_2 (506₂)を計算し、 H_{n-1} (506 _{$n-1$})の不可逆変換値 H_n (506 _{n})を計算するまで、 H_i の不可逆変換値 H_{i+1} ($1 \leq i < n$)を繰り返し計算する。

【0145】最後に、販売者100は、ステップ1103で作成したUID505と、 n 番目の不可逆変換値 H_n (506 _{n})とを、1枚目のチケットとして、消費者200に対して送信する(ステップ1106)。

【0146】図21は、図17および図18のチケット

受信処理(S2200)の処理フローチャートであり、本処理は、チケット要求・受信・発信処理プログラム207cによって実現される。

【0147】図21に示すように、チケット受信処理(S2200)において、消費者200は、販売者100から送信されてきたデータを受信すると(ステップ2201)、受信したデータにUID505が含まれているか否かを判定し(ステップ2202)、含まれている場合には、UID505を記憶装置205に保存する(ステップ2203)。

【0148】最後に、消費者200は、受信した不可逆変換値 H_m を記憶装置205に保存する(ステップ2204)。

【0149】なお、消費者200は、受信した不可逆変換値 H_m を記憶装置205に保存した回数をカウントすることで、何枚目のチケットが発券されたかを認識することができる。そこで、消費者端末201において、何枚目のチケットが発券されたかを示す表示が表示装置203になされるようにすることが好ましい。

【0150】図22は、図18のチケット発券要求処理(S2300)の処理フローチャートであり、本処理は、チケット要求・受信・発信処理プログラム207cによって実現される。

【0151】図22に示すように、チケット発券要求処理(S2300)において、消費者200は、まず、販売者100に対して、販売者100の公開鍵を要求し、公開鍵を受信する(ステップ2301)。

【0152】続いて、消費者200は、自身だけしか知らないパスワード(初期チケット発券要求処理(S2100)で入力したパスワードと同一のパスワード)を入力する(ステップ2302)。

【0153】続いて、消費者200は、ステップ2302で入力したパスワードを、ステップ2301で入手した公開鍵を用いて暗号化し(ステップ2303)、暗号化したパスワード501と、図21に示したチケット受信処理(S2200)で入手したUID505と、1回前のチケット受信処理(S2200)で入手した不可逆変換値 H_m とを、販売者100に対して送信する(ステップ2304)。

【0154】このように、1回前のチケット受信処理(S2200)で入手した不可逆変換値 H_m を送信することによって、販売者100は、消費者200が発券した最新のチケットが何枚目であるか、すなわち、消費者200が何枚目までのチケットを集めているかを知ることができる。

【0155】なお、消費者200は、1枚目のチケットの発券を要求すべきであるか(図19に示した初期チケット発券要求処理(S2100)を行うべきであるか)、または、2枚目以降のチケットの発券を要求すべきであるか(図22に示したチケット発券要求処理(S

2300)を行うべきであるか)については、記憶装置205にUID505が記憶されているか否かで判断することができる。

【0156】図23は、図18のチケット発券処理(S1200)の処理フローチャートであり、本処理は、チケット発券・検証処理プログラム107cによって実現される。

【0157】図23に示すように、チケット発券処理(S1200)において、販売者100は、まず、暗号化されたパスワード501、UID505、不可逆変換値 H_0 を受信すると(ステップ1201)、受信したパスワード501を、販売者100の秘密鍵を用いて復号する(ステップ1202)。ここでは、公開鍵暗号技術を使ってパスワードを暗号化する例を示しているが、パスワードが通信網300を通過する際に盗聴されなければ、どのような暗号技術を使ってもかまわない。

【0158】続いて、販売者100は、ステップ1202で復号したパスワード、ステップ1201で受信したUID505、販売者100の秘密鍵を結合したものの、不可逆変換値 H_1 を計算する(ステップ1203)。

【0159】続いて、販売者100は、ステップ1201で受信した H_0 とステップ1203で計算した H_1 とが一致するか否かを検証し(ステップ1204)、一致した場合は、消費者200が n 枚のチケットを集め終えたことを意味しているので、ステップ1208に進んで、チケット収集完了処理を行う。なお、ステップ1208のチケット収集完了処理は、図18のチケット収集終了処理(S1250)に相当しており、その処理内容は、販売者100の販売方針に応じた様々な処理内容が考えられ、特に定めるものではない。

【0160】また、販売者100は、ステップ1201で受信した H_0 とステップ1203で計算した H_1 とが一致しない場合は(ステップ1204)、消費者200が n 枚のチケットを集め終えていないことを意味しているので、 H_i の不可逆変換値 H_{i+1} ($1 \leq i < n$)を計算し(ステップ1205)、 $H_0 = H_i$ となる i ($1 < i \leq n$)を求める(ステップ1206)。なお、ステップ1206では、販売者100は、図20に示した初期チケット発券処理(S1100)のステップ1105と同様にして、 H_i の不可逆変換値 H_{i+1} ($1 \leq i < n$)を繰り返し計算するが、 $H_0 = H_i$ となる i ($1 < i \leq n$)が求まった時点で、計算を中止することができる。

【0161】ここで、 $H_0 = H_i$ となる i が存在しない場合は、ステップ1201で受信したパスワード501、UID505、 H_m の少なくともいずれかが不正であることを意味しているので、エラー処理を実行する(ステップ1209)。

【0162】また、販売者100は、 $H_0 = H_i$ となる i が存在する場合は、UID505と共に、 H_{i-1} を、消

費者200に対して送信する(ステップ1207)。

【0163】以上説明したように、第2の実施形態に係る電子クーポンシステムにおいては、チケットの発券時に、販売者100だけしか知らない秘密の情報である販売者100の秘密鍵、消費者200だけしか知らない情報であるパスワード、 n 枚のチケットの組を識別するためのUIDを連結したものから、不可逆変換値を繰り返し計算し、 n 番目の不可逆変換値 H_n 、 $n-1$ 番目の不可逆変換値 H_{n-1} 、 \dots 、2番目の不可逆変換値 H_2 、1番目の不可逆変換値 H_1 という順番で、各不可逆変換値を消費者200に対して返信するようにしている。また、消費者200から販売者100に対して、1回前に送信された H_0 、UID、パスワードを送信するようにしている。また、不可逆変換値を計算するのに必要な消費者200ごとのデータは、消費者200から販売者100に対して送信されるようにしている。

【0164】従って、第2の実施形態に係る電子クーポンシステムによれば、上述した第1の実施形態による効果に加えて、たとえチケットが通信路上で盗まれたとしても、パスワードを知らない第三者がチケットを不正使用するのを防止することができると共に、販売者100側で、消費者200ごとに既に何枚のチケットを発券したかを管理する必要がなくなる。

【0165】なお、第2の実施形態に係る電子クーポンシステムにおいても、上述した第1の実施形態で説明したように、本発明の要旨の範囲内で様々な変形が可能である。

【0166】例えば、第2の実施形態に係る電子クーポンシステムにおいては、販売者100は、チケット発券時に、販売者100の秘密鍵を用いて不可逆変換値を計算するようにしているが、この計算は、販売者100以外が計算不可能であればよいので、不可逆変換のアルゴリズムが非公開であれば、販売者100の秘密鍵を用いなくてもよい。

【0167】また、第2の実施形態に係る電子クーポンシステムにおいては、販売者100が、初期チケット発券時に、消費者200に対してUIDを送信し、消費者200が、そのUIDを保管しておき、その後は、保管しておいたUIDを消費者200から販売者100に対して送信するようにしているが、チケット発券時に、その都度、販売者100から消費者200に対してUIDを送信するようにしてもよい。

【0168】また、第2の実施形態に係る電子クーポンシステムにおいては、販売者100は、チケット発券時に、販売者100の秘密鍵、パスワード、UIDを連結したものから計算した不可逆変換値を、消費者200に対して返信するようにしているが、パスワードおよびUIDを連結したものを、販売者100だけしか知らない秘密の暗号鍵(例えば、公開鍵暗号方式における販売者100の秘密鍵)を用いて暗号化し、暗号化した暗号化

情報を、消費者200に対して返信するようにしてもよい。詳しくは、販売者100は、パスワードおよびUIDを連結したものの暗号化情報 H_1 に基づいて、暗号化情報 H_i ($1 \leq i < n$) の暗号化情報 H_{i+1} を順次計算し、 n 番目の暗号化情報 H_n 、 $n-1$ 番目の暗号化情報 H_{n-1} 、 \dots 、2番目の暗号化情報 H_2 、1番目の暗号化情報 H_1 という順番で、各暗号化情報を消費者200に対して返信するようにしてもよい。

【0169】また、第2の実施形態に係る電子クーポンシステムにおいては、販売者100は、チケット発券時に、販売者100の秘密鍵、パスワード、UIDを連結したもののから計算した不可逆変換値を、消費者200に対して返信するようにしているが、パスワード、UID、何枚目のチケットであるかを示す枚数情報を連結したものを、販売者100だけしか知らない秘密の暗号鍵（例えば、公開鍵暗号方式における販売者100の秘密鍵）を用いて暗号化し、暗号化した暗号化情報を、消費者200に対して返信するようにしてもよい。このようにすれば、販売者100は、消費者200からチケットの発券要求時に送信されてくる暗号化情報を、販売者100だけしか知らない秘密の暗号鍵を用いて復号した結果得られる枚数情報によって、消費者200が何枚のチケットを集めたかを知ることができる。

【0170】また、第2の実施形態に係る電子クーポンシステムにおいては、販売者100は、チケット発券時に、不可逆変換値を消費者200に対して送信するようにしているが、上述した第1の実施形態で説明したクーポンと同様に、不可逆変換値を目視可能なデータとして記載したチケットを作成し、書面としてのチケットを消費者200に対して送信するようにしてもよい。このようにすれば、消費者端末201においては、例えば、図25に示すような表示が表示装置203になされて、何枚目のチケットが発券されたかを示すようにすることができる。

【0171】さらに、第2の実施形態に係る電子クーポンシステムにおいても、上述した第1の実施形態で説明したクーポンと同様に、販売者100から消費者200に対して、チケットと共に、チケット全体のデジタル署名が送信されるようにしてもよく、このようにすれば、チケットの発券を受けた消費者200側で、受け取ったチケットが改ざんされていないか否かを検証することができる。

【0172】（第3の実施形態）ところで、クーポンの発券を、販売者100とは別に設けた専用の発券者が行うようにしてもよく、以下、クーポンの発券者を設けるようにした場合を、第3の実施形態として、上述した第1の実施形態と異なる点についてのみ説明する。

【0173】図26は、第3の実施形態に係る電子クーポンシステムの概略構成を示す図である。

【0174】第3の実施形態に係る電子クーポンシステム

は、消費者200₁～200_n（以下、単に「消費者200」とも称す。）、販売者端末600₁～600_n（以下、単に「販売者600」とも称す。）、発券者700が利用するシステムであり、図26に示すように、消費者200が利用する端末である消費者端末201₁～201_n（以下、単に「消費者端末201」とも称す。）と、販売者600が利用する端末である販売者端末601₁～601_n（以下、単に「販売者端末601」とも称す。）と、発券者700が利用する端末である発券者端末701とが、インターネット等の通信網300を介して互いに接続されて構成されている。

【0175】次に、第3の実施形態に係る電子クーポンシステムを構成する発券者端末701および販売店端末601のハードウェア構成について、図27および図28を用いて説明する。なお、消費者端末201のハードウェア構成は、図3に示したハードウェア構成と同様である。

【0176】図27は発券者端末701のハードウェア構成を示す図である。

【0177】図27に示すように、発券者端末701は、通信インタフェース702と、表示装置703と、入力装置704と、記憶装置705と、中央処理装置（CPU）706と、一時記憶装置（メモリ）707とが、バス710によって互いに接続された構成となっており、基本的には、図2に示した販売者端末101のハードウェア構成と同様である。

【0178】メモリ707には、OS707aや、クーポン発券・検証処理プログラム707bといった、CPU706が実行するプログラム等が一時的に格納される。

【0179】ここで、OS707aは、発券者端末701全体の制御を行うために、ファイル管理、プロセス管理、デバイス管理といった機能を実現するためのプログラムである。また、クーポン発券・検証処理プログラム707bは、消費者200に対してクーポンを発券したり、販売者600から検証（後述するように、クーポンの二重使用についての検証である。）が要求されたクーポンを検証したりするためのプログラムである。

【0180】図28は販売者端末601のハードウェア構成を示す図である。

【0181】図2に示したハードウェア構成と異なる点は、メモリ107に、クーポン発券・検証処理プログラム107bの代わりに、クーポン検証処理プログラム607bが一時的に格納される点である。

【0182】クーポン検証処理プログラム607bは、消費者200から使用が要求されたクーポンを検証するためのプログラムである。

【0183】次に、第3の実施形態に係る電子クーポンシステムの動作について説明する。

【0184】なお、以下の説明においても、上述した第1

の実施形態と同様に、消費者200が行う処理は、実際には、消費者200の指示によって消費者端末201が実行し、販売者600が行う処理は、実際には、販売者600の指示によって販売者端末601が実行するものであり、さらに、発券者700が行う処理は、実際には、発券者700の指示によって発券者端末701が実行するものである。

【0185】図29は、消費者200が、発券者700に対してクーポンの発券を要求し、発券者700によって発券されたクーポンを受信するまでの動作を説明するための図である。

【0186】図29において、まず、消費者200は、発券者700からクーポンの発券を受ける条件を満たしているものとする(S2000)。

【0187】消費者200は、後述するクーポン要求処理(S12400)を行い、暗号化した自身のパスワード501を、発券者700に対して送信する。

【0188】発券者700は、パスワード501を受信すると、後述するクーポン発券処理(S7300)を行い、クーポン502と、クーポン502のデジタル署名503とを、消費者200に対して送信する。

【0189】消費者200は、クーポン502およびデジタル署名503を受信すると、後述するクーポン受信処理(S12500)を行い、受信したクーポン502を保管する。

【0190】図29に示した動作は、図4に示した動作において、販売者100が発券者700に代わっている点が異なる。

【0191】すなわち、図29のクーポン要求処理(S12400)の処理フローチャートは、図7に示したクーポン要求処理(S2400)の処理フローチャートと同様であるが、販売者100の公開鍵の代わりに発券者700の公開鍵を用いる点と、暗号化したパスワード501の送信先が、販売者100の代わりに発券者700となる点とが異なる。

【0192】また、図29のクーポン発券処理(S7300)の処理フローチャートは、図8に示したクーポン発券処理(S1300)の処理フローチャートと同様であるが、本処理を発券者700が行う点(本処理がクーポン発券・検証処理プログラム707bによって実現される点)と、販売者100の秘密鍵の代わりに発券者700の秘密鍵を用いる点とが異なる。

【0193】また、図29のクーポン受信処理(S12500)の処理フローチャートは、図9に示したクーポン受信処理(S2500)の処理フローチャートと同様である。

【0194】図30は、既にクーポンの発券を受けている消費者200が、通信網300を介してクーポンを使用し、販売者600が、クーポンを検証するまでの動作を説明するための図である。

【0195】図30において、既にクーポンの発券を受けている消費者200は、クーポン使用オンライン処理(S2600)を行い、クーポン受信処理(S12500)で入手したクーポン502と、暗号化した自身のパスワード501とを、販売者600に対して送信する。

【0196】販売者600は、クーポン502およびパスワード501を受信すると、後述するクーポン検証処理(S6400)を行い、受信したクーポン502を検証する。

【0197】図31は、既にクーポンの発券を受けている消費者200が、クーポンを印刷し、印刷されたクーポンを販売店に持参して使用し、販売者600が、クーポンを検証するまでの動作を説明するための図である。

【0198】図31において、既にクーポンの発券を受けている消費者200は、クーポン使用オフライン処理(S2700)を行い、印刷されたクーポン504を販売店に持参する。

【0199】販売者600は、消費者200が持参したクーポン504を受け取ると、後述するクーポン検証処理(S6400)を行い、受け取ったクーポン504を検証する。

【0200】図30および図31に示した動作は、各々、図5および図6に示した動作において、販売者600が行うクーポン検証処理(S6400)の処理内容のみが異なり、本処理の処理内容については後述する。

【0201】すなわち、図30のクーポン使用オンライン処理(S2600)の処理フローチャートは、図10に示したクーポン使用オンライン処理(S2600)の処理フローチャートと同様である。

【0202】また、図31のクーポン使用オフライン処理(S2700)の処理フローチャートは、図11に示したクーポン使用オフライン処理(S2700)の処理フローチャートと同様である。

【0203】図32は、図30および図31のクーポン検証処理(S6400)の処理フローチャートであり、本処理は、クーポン検証処理プログラム607bによって実現される。

【0204】図32に示すように、クーポン検証処理(S6400)においては、販売者600は、図12に示したクーポン検証処理(S1200)と同様の処理を行うが、ステップ11404の書面検証処理の処理内容が、後述するように異なる。

【0205】また、販売者600は、使用済みシリアル番号リストを管理せず、ステップ11406で、クーポンに記載されているシリアル番号を発券者700に対して通知し、使用済みシリアル番号リストへのシリアル番号の登録を発券者700に行ってもらっている点が異なる。

【0206】図33は、図32の書面検証処理(ステップ11404)の処理フローチャートである。

【0207】図33に示すように、書面検証処理（ステップ11404）においては、販売者600は、図13に示した書面検証処理と同様の処理を行うが、ステップ11410で、クーポンに記載されているデジタル署名を、発券者700の公開鍵を用いて復号している点と、ステップ11414で、クーポンに記載されているシリアル番号を発券者700に対して通知し、使用済みシリアル番号リストにシリアル番号が登録されているか否かを発券者700に問い合わせるようにしている点とが異なる。そこで、販売者600は、ステップ1411の検証では、ステップ11410で復号した結果と、クーポンに記載されているクーポン情報とを比較することとなる。

【0208】以上説明したように、第3の実施形態に係る電子クーポンシステムにおいても、上述した第1の実施形態と同様に、シリアル番号、有効期限、金額等の改ざんされては困るクーポン情報のデジタル署名を、発券者700だけしか知らない情報である秘密鍵を用いて計算し、計算したデジタル署名を、目視可能なデータとして記載したクーポンを作成するようにしている。

【0209】従って、第3の実施形態に係る電子クーポンシステムによれば、上述した第1の実施形態と同様に、消費者200が電子的なクーポンを印刷して使用する場合でも、印刷されたクーポンに記載されているデジタル署名を検証することで、クーポンの偽造や改ざんを検出することができる。

【0210】なお、第3の実施形態に係る電子クーポンシステムでは、デジタル署名を作成する発券者700と、デジタル署名を検証する販売者600とが異なるが、デジタル署名の作成時に発券者700の秘密鍵を用い、デジタル署名の検証時に発券者700の公開鍵を用いるようにすることで、販売者600によるデジタル署名の検証が可能である。ただし、販売者600および発券者700の双方だけしか知らない秘密の暗号鍵を用いて、クーポン情報を暗号化し、暗号化した暗号化情報を、目視可能なデータとしてクーポンに記載するようにしても、販売者600による暗号化情報の検証は可能である。

【0211】また、第3の実施形態に係る電子クーポンシステムにおいても、上述した第1の実施形態と同様に、クーポンの発券時に、消費者200が提示したパスワードの不可逆変換値を、目視可能なデータとして記載したクーポンを作成するようにしている。さらに、クーポンの使用時には、発券を要求した消費者200だけしか知らないパスワードを販売者600に提示し、消費者200が提示したパスワードの不可逆変換値と、クーポンに記載されている不可逆変換値とを比較するようにしている。

【0212】従って、第3の実施形態に係る電子クーポンシステムによれば、上述した第1の実施形態と同様

に、たとえクーポンが盗まれたとしても、クーポンの発券要求時に提示されたパスワードを知らない第三者がクーポンを不正使用するのを防止することができる。

【0213】なお、第3の実施形態に係る電子クーポンシステムにおいては、パスワードについて、不可逆変換を施した不可逆変換値を、目視可能なデータとしてクーポンに記載するようにした例を示しており、本例によれば、不可逆変換方法を公開しても支障がないので、販売者600による不可逆変換値の検証が可能であると共に、パスワードの不可逆変換値が不一致である場合に、消費者200が、自身が提示したパスワードの不可逆変換値を計算して確認することが可能である。しかしながら、パスワードについて、販売者600および発券者700の双方だけしか暗号化できない暗号化方法で暗号化した暗号化情報を、目視可能なデータとしてクーポンに記載するようにしても、販売者600による暗号化情報の検証は可能である。

【0214】なお、第3の実施形態に係る電子クーポンシステムにおいても、上述した第1の実施形態で説明したように、本発明の要旨の範囲内で様々な変形が可能である。

【0215】例えば、第3の実施形態に係る電子クーポンシステムにおいては、消費者200は、発券者700および販売者600に対してパスワードを送信するときに、発券者700および販売者600の公開鍵を取得し、暗号通信を行うようにしているが、本発明はこれに限定しない。消費者200は、1度、発券者700および販売者600の公開鍵を入手すれば、2回以降は、その公開鍵を使うことができる。また、発券者700および販売者600と消費者200との間で共通の鍵を持つことができれば、秘密鍵暗号技術を使って暗号化するようにしてもよい。

【0216】また、第3の実施形態に係る電子クーポンシステムにおいて、消費者200から発券者700および販売者600に対してパスワードを送信するときに、暗号化されたパスワードがそのまま盗まれて不正使用されるのを防止するために、パスワードを、その他の情報（乱数や適当な数字でよい。）と共に暗号化して送信するようにしてもよい。

【0217】また、第3の実施形態に係る電子クーポンシステムにおいては、発券者700は、デジタル署名を、数値や文字等の目視可能なデータとしてクーポンに記載するようにしているが、印刷後に目視可能であれば、例えば、バーコード等のようなものであってもよい。バーコードとして記載すれば、販売者600は、印刷されたクーポンから各種情報を取得する際に、バーコードリーダを用いることができるようになる。

【0218】また、第3の実施形態に係る電子クーポンシステムにおいては、発券者700は、消費者200のパスワードの不可逆変換値と、シリアル番号、有効期

限、金額等のクーポン情報のデジタル署名とを、別々にクーポンに記載するようにしているが、クーポン情報と共に、パスワードも一緒にデジタル署名を計算するようにしてもよい。また、このとき、クーポン情報やパスワード等の、デジタル署名を計算する元の情報は、不可逆変換を施した後に、デジタル署名を計算するようにしてもよい。

【0219】また、第3の実施形態に係る電子クーポンシステムにおいては、消費者200から使用が要求されたクーポンを販売者600が検証し、クーポンの二重使用のみを発券者700が一元管理して検証する方法を取っているが、販売者600が受け取ったクーポンを、そのときに提示されたパスワードと共に発券者700に提示し、発券者700側でクーポンを検証するようにしてもよい。また、その両方を組み合わせるようにしてもよい。

【0220】発券者700側でクーポンを検証するようにすれば、発券者700だけしか知らない秘密の暗号鍵を用いてクーポン情報を暗号化した暗号化情報を、目視可能なデータとしてクーポンに記載するようにし、この暗号化情報を検証するようにすることができる。また、発券者700だけしか暗号化できない暗号化方法でパスワードを暗号化した暗号化情報を、目視可能なデータとしてクーポンに記載するようにし、この暗号化情報を検証するようにすることもできる。

【0221】(第4の実施形態)ところで、上述した第3の実施形態に係る電子クーポンシステムにおいて、発券者700は、上述した第2の実施形態で説明したように、チケットを取り扱うようにすることができ、そのようにした場合を、第4の実施形態として、上述した第2の実施形態および第3の実施形態と異なる点についてのみ説明する。

【0222】第4の実施形態に係る電子クーポンシステムの概略構成は、図26に示した概略構成と同様である。

【0223】図34は発券者端末701のハードウェア構成を示す図である。

【0224】図27に示したハードウェア構成と異なる点は、メモリ707に、チケット発券・検証処理プログラム707cが一時的に格納される点である。

【0225】チケット発券・検証処理プログラム707cは、消費者200に対してチケットを発券したり、消費者200から使用が要求されたチケットを検証したりするためのプログラムである。

【0226】なお、販売者端末601のハードウェア構成は、図28に示したハードウェア構成と同様であり、消費者端末201のハードウェア構成は、図16に示したハードウェア構成と同様である。

【0227】次に、第4の実施形態に係る電子クーポンシステムの動作について説明する。

【0228】なお、以下の説明においても、上述した第3の実施形態と同様に、消費者200が行う処理は、実際には、消費者200の指示によって消費者端末201が実行し、発券者700が行う処理は、実際には、発券者700の指示によって発券者端末701が実行するものである。

【0229】図35は、消費者200が、発券者700に対して1枚目のチケットの発券を要求し、発券者700によって発券された1枚目のチケットを受信するまでの動作を説明するための図である。なお、チケットは、n枚だけ集めたときに効力を発揮するものとする。

【0230】図35において、まず、消費者200は、後述する初期チケット発券要求処理(S12100)を行い、暗号化した自身のパスワード501を、発券者700に対して送信する。

【0231】発券者700は、パスワード501を受信すると、後述する初期チケット発券処理(S7100)を行い、n枚のチケットの組を識別するために付与した固有の値(以下、「UID」と称す。)505と、受信したパスワード501、UID505、発券者700だけしか知らない秘密の情報(例えば、発券者700の秘密鍵)を連結したものの、n番目の不可逆変換値 $H_n(506_n)$ とを、1枚目のチケットとして、消費者200に対して送信する。

【0232】消費者200は、UID505および $H_n(506_n)$ を受信すると、後述するチケット受信処理(S12200)を行い、受信したUID505および $H_n(506_n)$ を保管する。

【0233】図35に示した動作は、図17に示した動作において、販売者100が発券者700に代わっている点異なる。

【0234】すなわち、図35の初期チケット発券要求処理(S12100)の処理フローチャートは、図19に示した初期チケット発券要求処理(S2100)の処理フローチャートと同様であるが、販売者100の公開鍵の代わりに発券者700の公開鍵を用いる点と、暗号化したパスワード501の送信先が、販売者100の代わりに発券者700となる点とが異なる。

【0235】また、図35の初期チケット発券処理(S7100)の処理フローチャートは、図20に示した初期チケット発券処理(S1100)の処理フローチャートと同様であるが、本処理を発券者700が行う点(本処理がチケット発券・検証処理プログラム707cによって実現される点)と、販売者100の秘密鍵の代わりに発券者700の秘密鍵を用いる点とが異なる。

【0236】また、図35のチケット受信処理(S12200)の処理フローチャートは、図21に示したチケット受信処理(S2200)の処理フローチャートと同様である。

【0237】図36は、消費者200が、発券者700

に対して2枚目以降のチケットの発券を要求し、発券者700によって発券された2枚目以降のチケットを受信するまでの動作を説明するための図である。

【0238】図36において、まず、消費者200は、2枚目のチケットの発券を受ける場合は、後述するチケット発券要求処理(S12300)を行い、暗号化した自身のパスワード501と、1枚目のチケット受信処理(S12200)で入手したUID505および $H_n(506_n)$ とを、発券者700に対して送信する。

【0239】発券者700は、パスワード501、UID505、 $H_n(506_n)$ を受信すると、後述するチケット発券処理(S7200)を行い、受信したパスワード501、UID505、 $H_n(506_n)$ と、発券者700の秘密鍵とから、 $H_{n-1}(506_{n-1})$ を求めて、求めた $H_{n-1}(506_{n-1})$ を、2枚目のチケットとして、消費者200に対して送信する。

【0240】消費者200は、 $H_{n-1}(506_{n-1})$ を受信すると、チケット受信処理(S122200)を行い、受信した $H_{n-1}(506_{n-1})$ を保管する。

【0241】同様に、消費者200は、 $m+1$ 枚目($1 \leq m < n$)のチケットの発券を受ける場合は、チケット発券要求処理(S12300)を行い、暗号化した自身のパスワード501と、 m 枚目のチケット受信処理(S12200)で入手したUID505および $H_{n-(m-1)}(506_{n-(m-1)})$ とを、発券者700に対して送信する。

【0242】発券者700は、パスワード501、UID505、 $H_{n-(m-1)}(506_{n-(m-1)})$ を受信すると、チケット発券処理(S7200)を行い、受信したパスワード501、UID505、 $H_{n-(m-1)}(506_{n-(m-1)})$ と、発券者700の秘密鍵とから、 $H_{n-m}(506_{n-m})$ を求めて、求めた $H_{n-m}(506_{n-m})$ を、 $m+1$ 枚目のチケットとして、消費者200に対して送信する。

【0243】消費者200は、 $H_{n-m}(506_{n-m})$ を受信すると、チケット受信処理(S122200)を行い、受信した $H_{n-m}(506_{n-m})$ を保管する。

【0244】このようにして、消費者200は、 n 枚のチケットを集めることができ、これら n 枚のチケットの効力を発揮させたい場合には、チケット発券要求処理(S12300)を行い、暗号化された自身のパスワード501と、 n 枚目のチケット受信処理(S12200)で入手したUID505および $H_1(506_1)$ とを、発券者700に対して送信する。

【0245】発券者700は、パスワード501、UID505、 $H_1(506_1)$ を受信すると、チケット発券処理(S7200)を行い、受信したパスワード501、UID505、 $H_1(506_1)$ と、発券者700の秘密鍵とから、消費者200が n 枚だけチケットを集めたことを確認し、 n 枚のチケット収集終了処理(S7250)を行う。

【0246】図36に示した動作は、図18に示した動作において、販売者100が発券者700に代わっている点異なる。

【0247】すなわち、図36のチケット発券要求処理(S12100)の処理フローチャートは、図22に示したチケット発券要求処理(S2300)の処理フローチャートと同様であるが、販売者100の公開鍵の代わりに発券者700の公開鍵を用いる点と、暗号化したパスワード501、保存しているUID505および H_n の送信先が、販売者100の代わりに発券者700となる点とが異なる。

【0248】また、図36のチケット発券処理(S7100)の処理フローチャートは、図23に示したチケット発券処理(S1200)の処理フローチャートと同様であるが、本処理を発券者700が行う点(本処理がチケット発券・検証処理プログラム707cによって実現される点)と、販売者100の秘密鍵の代わりに発券者700の秘密鍵を用いる点とが異なる。

【0249】また、図36のチケット受信処理(S12200)の処理フローチャートは、図21に示したチケット受信処理(S2200)の処理フローチャートと同様である。

【0250】なお、チケットを n 枚だけ集めたときに発揮する効力は、販売者100の販売方針に応じて異なるようにすることができるが、チケットを n 枚だけ集めたか否かの判定を、発券者700が行うようにしているので、図36のチケット収集終了処理(S7250)は、発券者700が行うものとしている。

【0251】以上説明したように、第4の実施形態に係る電子クーポンシステムにおいても、上述した第2の実施形態と同様に、チケットの発券時に、発券者700だけしか知らない秘密の情報である発券者700の秘密鍵、消費者200だけしか知らない情報であるパスワード、 n 枚のチケットの組を識別するためのUIDを連結したものから、不可逆変換値を繰返し計算し、 n 番目の不可逆変換値 H_n 、 $n-1$ 番目の不可逆変換値 H_{n-1} 、…、2番目の不可逆変換値 H_2 、1番目の不可逆変換値 H_1 という順番で、各不可逆変換値を消費者200に対して返信するようにしている。また、消費者200から発券者700に対して、1回前に送信された H_n 、UID、パスワードを送信するようにしている。また、不可逆変換値を計算するのに必要な消費者200ごとのデータは、消費者200から発券者700に対して送信されるようにしている。

【0252】従って、第4の実施形態に係る電子クーポンシステムによれば、上述した第3の実施形態による効果に加えて、上述した第2の実施形態と同様に、たとえチケットが通信路上で盗まれたとしても、パスワードを知らない第三者がチケットを不正使用するのを防止することができると共に、発券者700側で、消費者200

ごとに既に何枚のチケットを発券したかを管理する必要がなくなる。

【0253】なお、第4の実施形態に係る電子クーポンシステムにおいても、上述した第3の実施形態で説明したように、本発明の要旨の範囲内で様々な変形が可能である。

【0254】例えば、第4の実施形態に係る電子クーポンシステムにおいては、発券者700は、チケット発券時に、発券者700の秘密鍵を用いて不可逆変換値を計算するようにしているが、この計算は、発券者700以外が計算不可能であればよいので、不可逆変換のアルゴリズムが非公開であれば、発券者700の秘密鍵を用いなくてもよい。

【0255】また、第4の実施形態に係る電子クーポンシステムにおいては、発券者700が、初期チケット発券時に、消費者200に対してUIDを送信し、消費者200が、そのUIDを保管しておき、その後は、保管しておいたUIDを消費者200から発券者700に対して送信するようにしているが、チケット発券時に、その都度、発券者700から消費者200に対してUIDを送信するようにしてもよい。

【0256】また、第4の実施形態に係る電子クーポンシステムにおいては、発券者700は、チケット発券時に、発券者700の秘密鍵、パスワード、UIDを連結したのから計算した不可逆変換値を、消費者200に対して返信するようにしているが、パスワードおよびUIDを連結したものを、発券者700だけしか知らない秘密の暗号鍵（例えば、公開鍵暗号方式における発券者700の秘密鍵）を用いて暗号化し、暗号化した暗号化情報を、消費者200に対して返信するようにしてもよい。詳しくは、発券者700は、パスワードおよびUIDを連結したものの暗号化情報 H_1 に基づいて、暗号化情報 H_i ($1 \leq i < n$) の暗号化情報 H_{i+1} を順次計算し、 n 番目の暗号化情報 H_n 、 $n-1$ 番目の暗号化情報 H_{n-1} 、 \dots 、2番目の暗号化情報 H_2 、1番目の暗号化情報 H_1 という順番で、各暗号化情報を消費者200に対して返信するようにしてもよい。

【0257】また、第4の実施形態に係る電子クーポンシステムにおいては、発券者700は、チケット発券時に、発券者700の秘密鍵、パスワード、UIDを連結したのから計算した不可逆変換値を、消費者200に対して返信するようにしているが、パスワード、UID、何枚目のチケットであるかを示す枚数情報を連結したものを、発券者700だけしか知らない秘密の暗号鍵（例えば、公開鍵暗号方式における発券者700の秘密鍵）を用いて暗号化し、暗号化した暗号化情報を、消費者200に対して返信するようにしてもよい。このようにすれば、発券者700は、消費者200からチケットの発券要求時に送信されてくる暗号化情報を、発券者700だけしか知らない秘密の暗号鍵を用いて復号した結

果得られる枚数情報によって、消費者200が何枚のチケットを集めたかを知ることができる。

【0258】また、第4の実施形態に係る電子クーポンシステムにおいては、発券者700は、チケット発券時に、不可逆変換値を消費者200に対して送信するようにしているが、上述した第1の実施形態で説明したクーポンと同様に、不可逆変換値を目視可能なデータとして記載したチケットを作成し、書面としてのチケットを消費者200に対して送信するようにしてもよい。

【0259】さらに、第4の実施形態に係る電子クーポンシステムにおいても、上述した第1の実施形態で説明したクーポンと同様に、発券者700から消費者200に対して、チケットと共に、チケット全体のデジタル署名が送信されるようにしてもよく、このようにすれば、チケットの発券を受けた消費者200側で、受け取ったチケットが改ざんされていないか否かを検証することができる。

【0260】

【発明の効果】以上説明したように、本発明によれば、電子的に発券されたクーポンが印刷されて使用される場合でも、クーポンの偽造や改ざん、第三者によるクーポンの不正使用を検出することができるようになるので、消費者は、電子的に発券されたクーポンを、ネットワーク上に開設されたバーチャル販売店だけではなく、現実存在する販売店でも使用することができるようになる。

【0261】さらに、本発明によれば、複数枚だけ集めたときに効力を発揮するチケットを取り扱う場合に、チケットを発券する側で消費者を管理する必要がなくなるので、チケットを発券する側の手間を減らすことができるようになる。

【図面の簡単な説明】

【図1】第1の実施形態に係る電子クーポンシステムの概略構成図。

【図2】第1の実施形態における販売者端末のハードウェア構成図。

【図3】第1の実施形態における消費者端末のハードウェア構成図。

【図4】第1の実施形態に係る電子クーポンシステムの動作のうち、消費者が、販売者に対してクーポンの発券を要求し、販売者によって発券されたクーポンを受信するまでの動作の説明図。

【図5】第1の実施形態に係る電子クーポンシステムの動作のうち、既にクーポンの発券を受けている消費者が、通信網を介してクーポンを使用し、販売者が、クーポンを検証するまでの動作の説明図。

【図6】第1の実施形態に係る電子クーポンシステムの動作のうち、既にクーポンの発券を受けている消費者が、クーポンを印刷し、印刷されたクーポンを販売店に持参して使用し、販売者が、クーポンを検証するまでの

動作の説明図。

【図7】図4のクーポン要求処理の処理フローチャート。

【図8】図4のクーポン発券処理の処理フローチャート。

【図9】図4のクーポン受信処理の処理フローチャート。

【図10】図5のクーポン使用オンライン処理の処理フローチャート。

【図11】図6のクーポン使用オフライン処理の処理フローチャート。

【図12】図5および図6のクーポン検証処理の処理フローチャート。

【図13】図12のステップ1404で行われる書面検証処理の処理フローチャート。

【図14】第1の実施形態に係る電子クーポンシステムで発券されるクーポンの形式の一例を示す説明図。

【図15】第2の実施形態における販売者端末のハードウェア構成図。

【図16】第2の実施形態における消費者端末のハードウェア構成図。

【図17】第2の実施形態に係る電子クーポンシステムの動作のうち、消費者が、販売者に対して1枚目のチケットの発券を要求し、販売者によって発券された1枚目のチケットを受信するまでの動作の説明図。

【図18】第2の実施形態に係る電子クーポンシステムの動作のうち、消費者が、販売者に対して2枚目以降のチケットの発券を要求し、販売者によって発券された2枚目以降のチケットを受信するまでの動作の説明図。

【図19】図17の初期チケット発券要求処理の処理フローチャート。

【図20】図17の初期チケット発券処理の処理フローチャート。

【図21】図17および図18のチケット受信処理の処理フローチャート。

【図22】図18のチケット発券要求処理の処理フローチャート。

【図23】図18のチケット発券処理の処理フローチャート。

【図24】図20のステップ1105で不可逆変換値が計算される様子を示す説明図。

【図25】第2の実施形態における消費者端末での表示の一例を示す説明図。

【図26】第3の実施形態に係る電子クーポンシステムの概略構成図。

【図27】第3の実施形態における発券者端末のハードウェア構成図。

【図28】第3の実施形態における販売者端末のハード

ウェア構成図。

【図29】第3の実施形態に係る電子クーポンシステムの動作のうち、消費者が、発券者に対してクーポンの発券を要求し、発券者によって発券されたクーポンを受信するまでの動作の説明図。

【図30】第3の実施形態に係る電子クーポンシステムの動作のうち、既にクーポンの発券を受けている消費者が、通信網を介してクーポンを使用し、販売者が、クーポンを検証するまでの動作の説明図。

【図31】第3の実施形態に係る電子クーポンシステムの動作のうち、既にクーポンの発券を受けている消費者が、クーポンを印刷し、印刷されたクーポンを販売店に持参して使用し、販売者が、クーポンを検証するまでの動作の説明図。

【図32】図30および図31のクーポン検証処理の処理フローチャート。

【図33】図32のステップ11404で行われる書面検証処理の処理フローチャート。

【図34】第4の実施形態における発券者端末のハードウェア構成図。

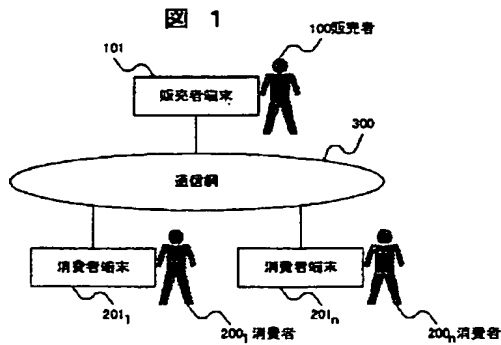
【図35】第4の実施形態に係る電子クーポンシステムの動作のうち、消費者が、発券者に対して1枚目のチケットの発券を要求し、発券者によって発券された1枚目のチケットを受信するまでの動作の説明図。

【図36】第4の実施形態に係る電子クーポンシステムの動作のうち、消費者が、発券者に対して2枚目以降のチケットの発券を要求し、発券者によって発券された2枚目以降のチケットを受信するまでの動作の説明図。

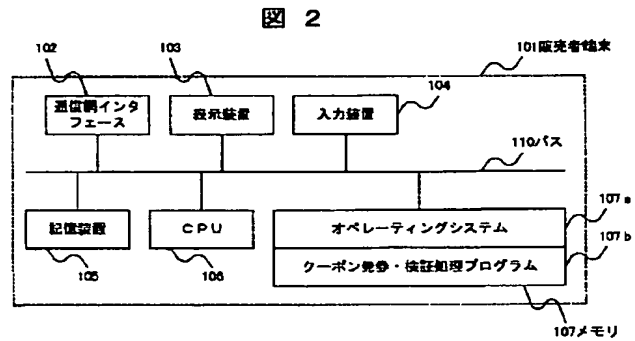
【符号の説明】

100, 600…販売者、200₁~200_n…消費者、700…発券者、101, 601₁~601_n…販売者端末、201₁~201_n…消費者端末、701…発券者端末、300…通信網、102, 202, 702…通信網インタフェース、103, 203, 703…表示装置、104, 204, 704…入力装置、105, 205, 705…記憶装置、106, 206, 706…中央処理装置(CPU)、107, 207, 707…一時記憶装置(メモリ)、208…印刷装置、110, 210, 710…バス、107a, 207a, 707a…オペレーティングシステム(OS)、107b, 707b…クーポン発券・検証処理プログラム、107c, 707c…チケット発券・検証処理プログラム、207b…クーポン要求・受信・発信処理プログラム、607b…クーポン検証処理プログラム、207c…チケット要求・受信・発信処理プログラム、501…パスワード、502…クーポン、503…デジタル署名、504…印刷されたクーポン、505…UID、506₁~506_n…不可逆変換値、507…秘密鍵。

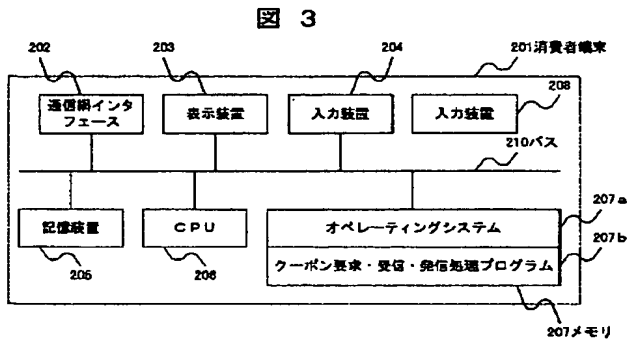
【図 1】



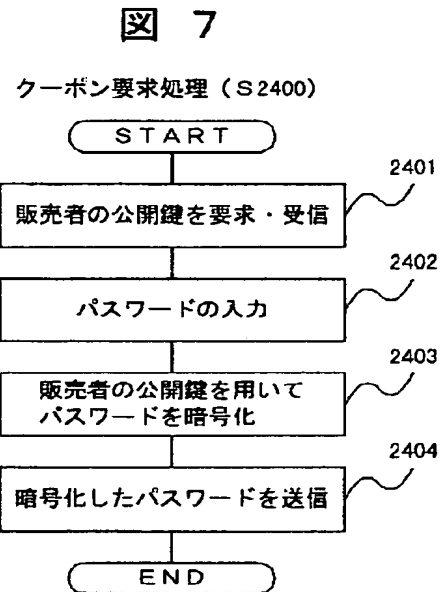
【図 2】



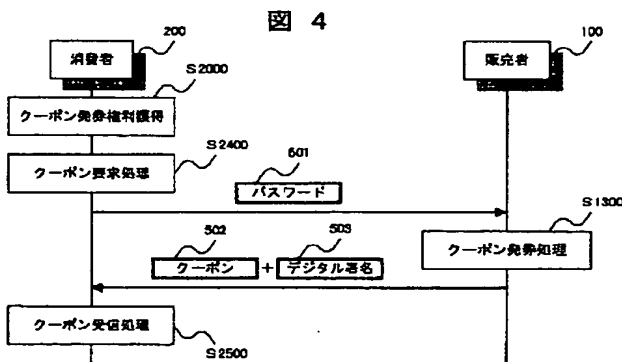
【図 3】



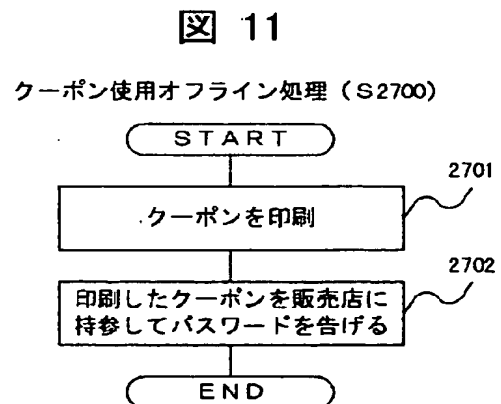
【図 7】



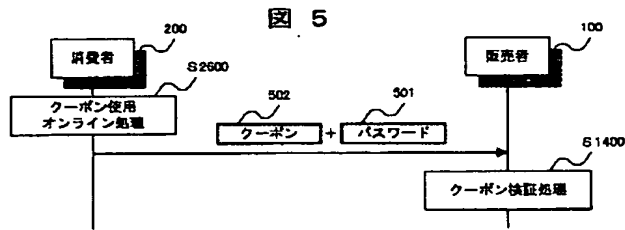
【図 4】



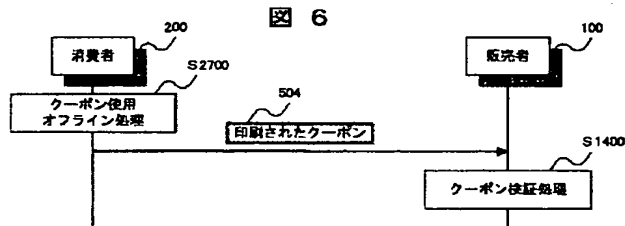
【図 11】



【図5】

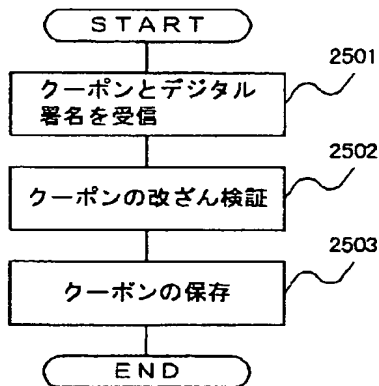


【図6】



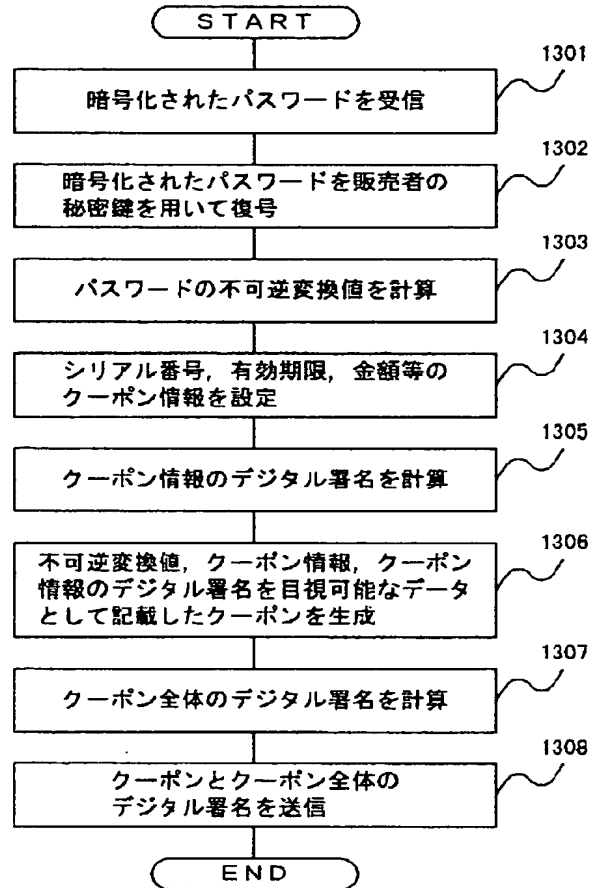
【図9】

図9
クーポン受信処理 (S2500)



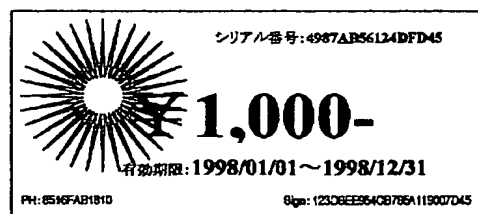
【図8】

図8
クーポン発券処理 (S1300)



【図14】

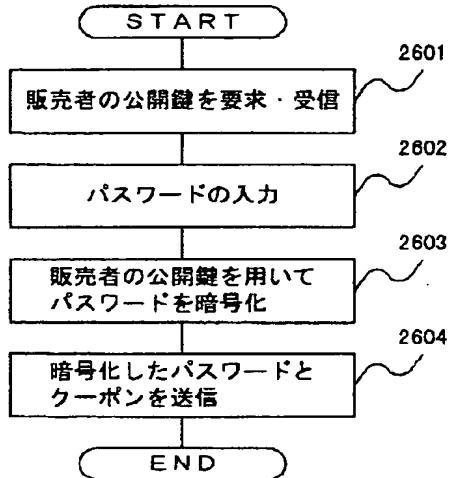
図14



【図10】

図 10

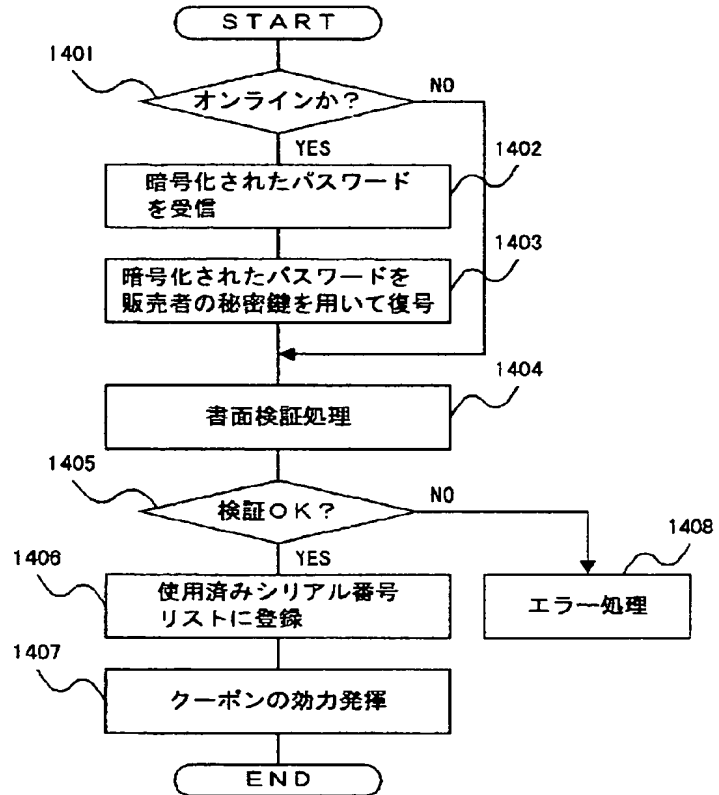
クーポン使用オンライン処理 (S2600)



【図12】

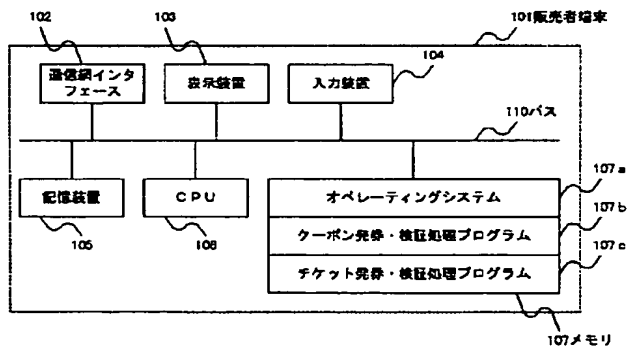
図 12

クーポン検証処理 (S1400)



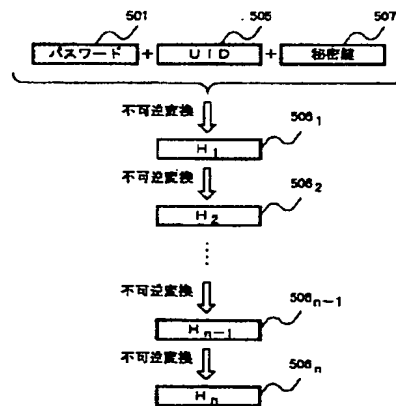
【図15】

図 15



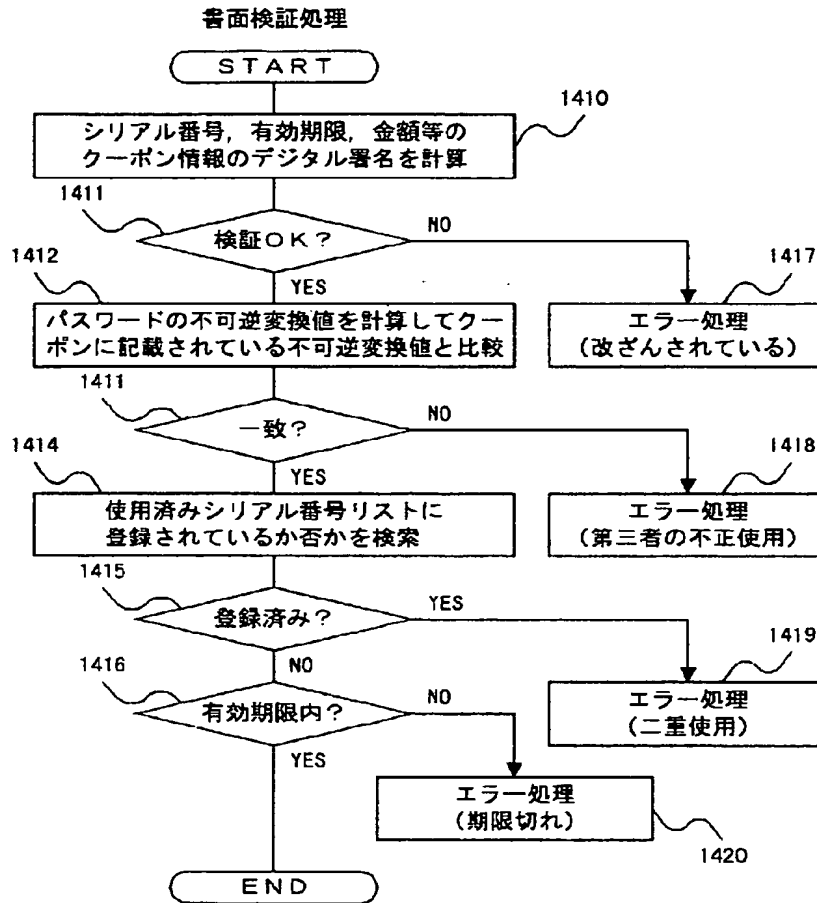
【図24】

図 24



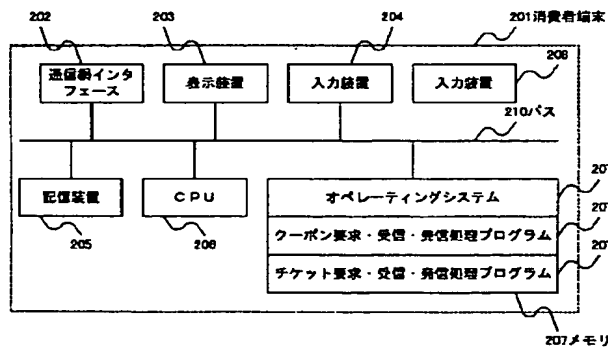
【図13】

図 13



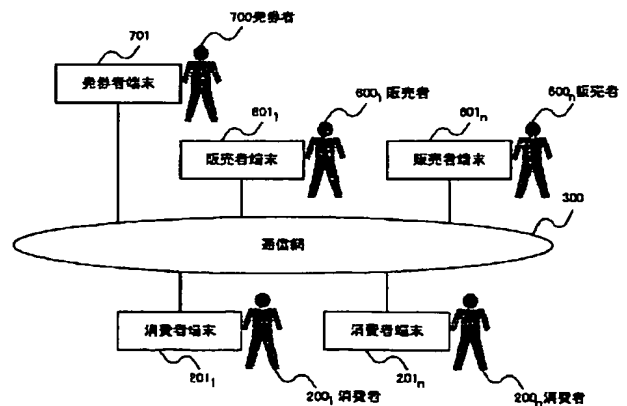
【図16】

図 16

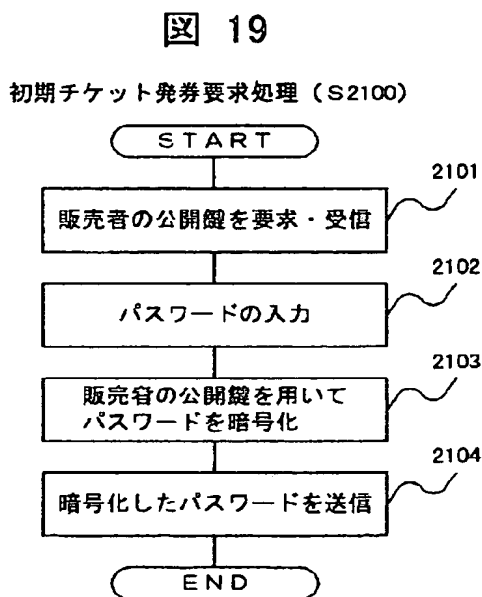


【図26】

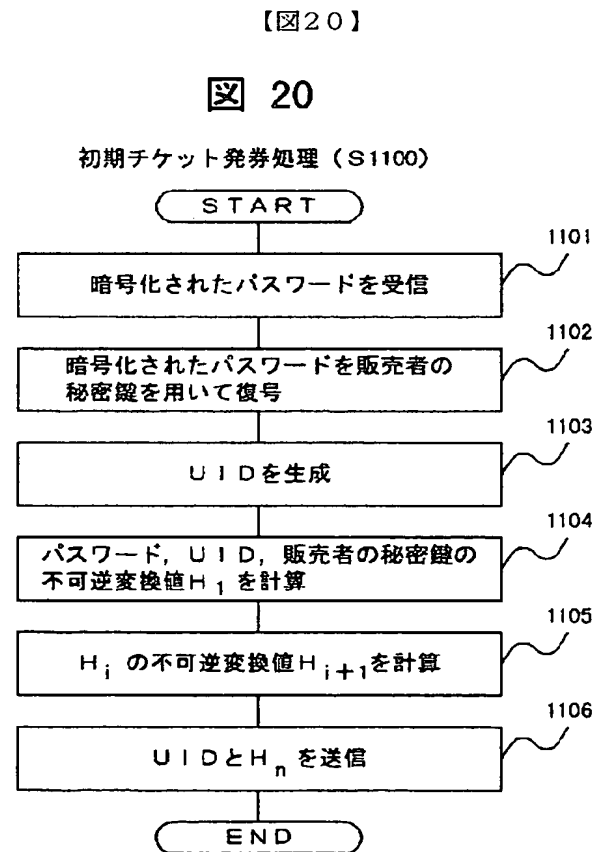
図 26



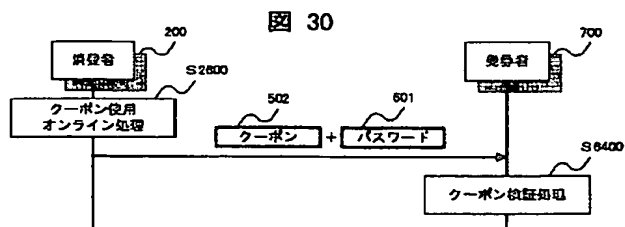
【图19】



【图20】

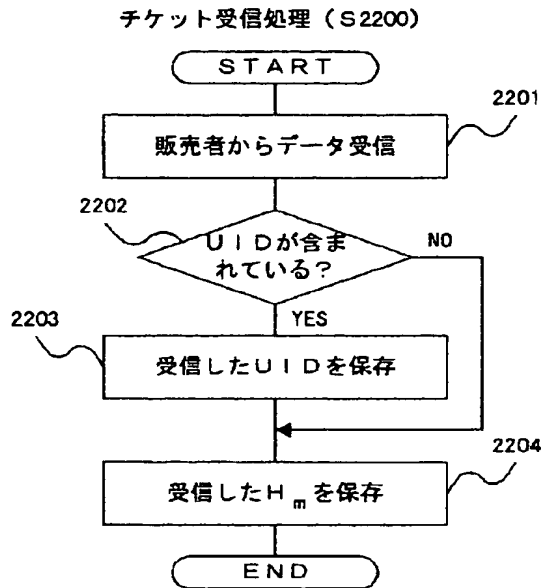


30



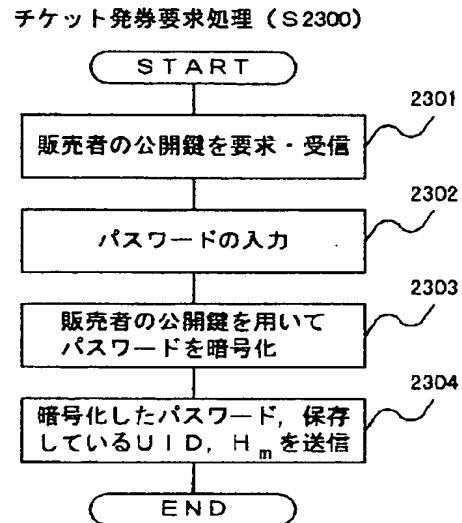
【図21】

図 21



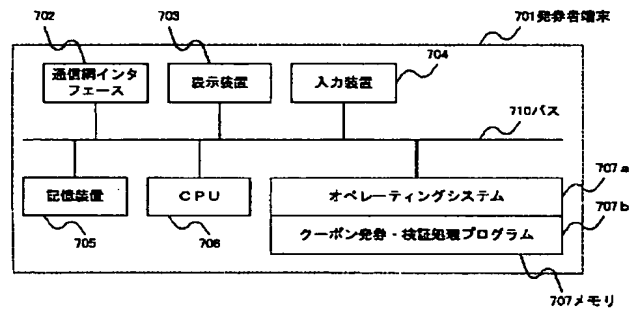
【図22】

図 22



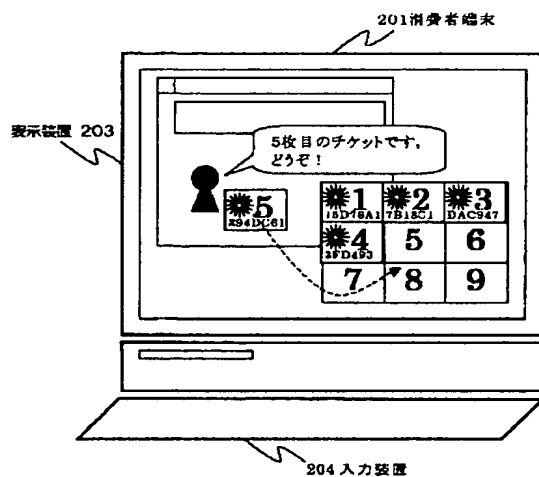
【図27】

図 27



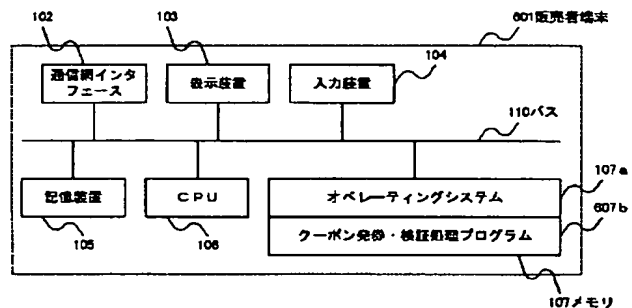
【図25】

図 25



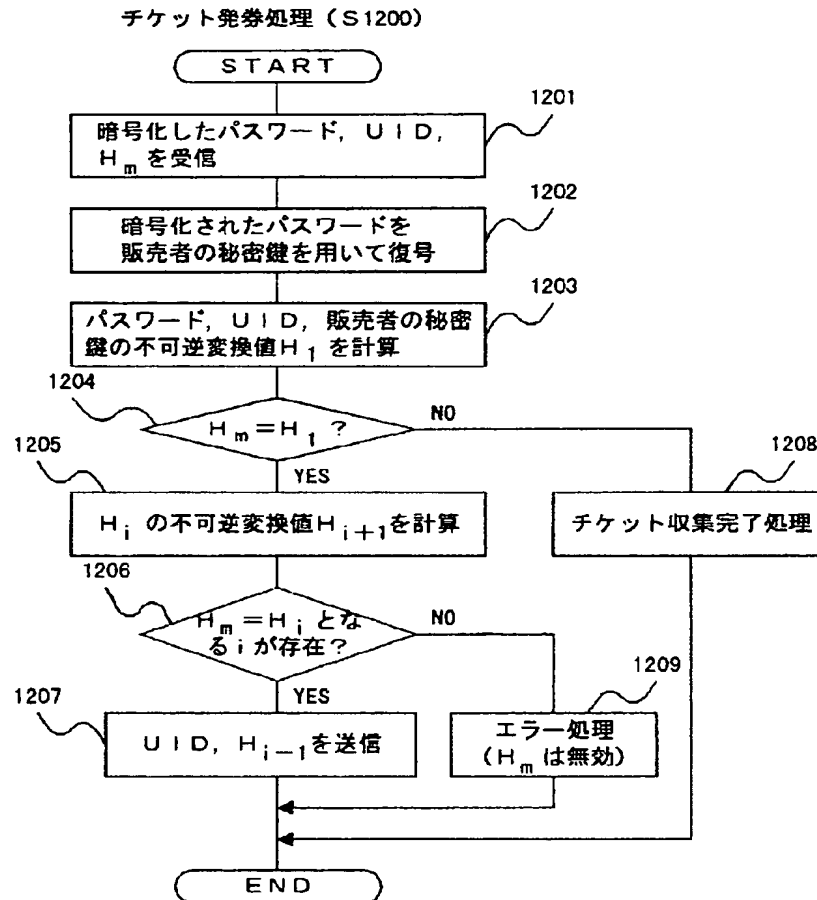
【図28】

図 28

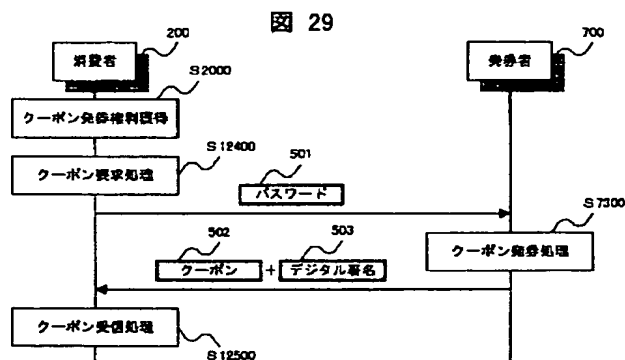


【図23】

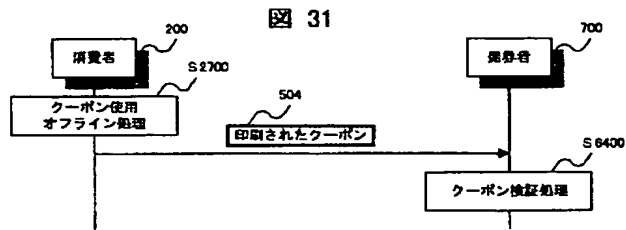
図 23



【図29】



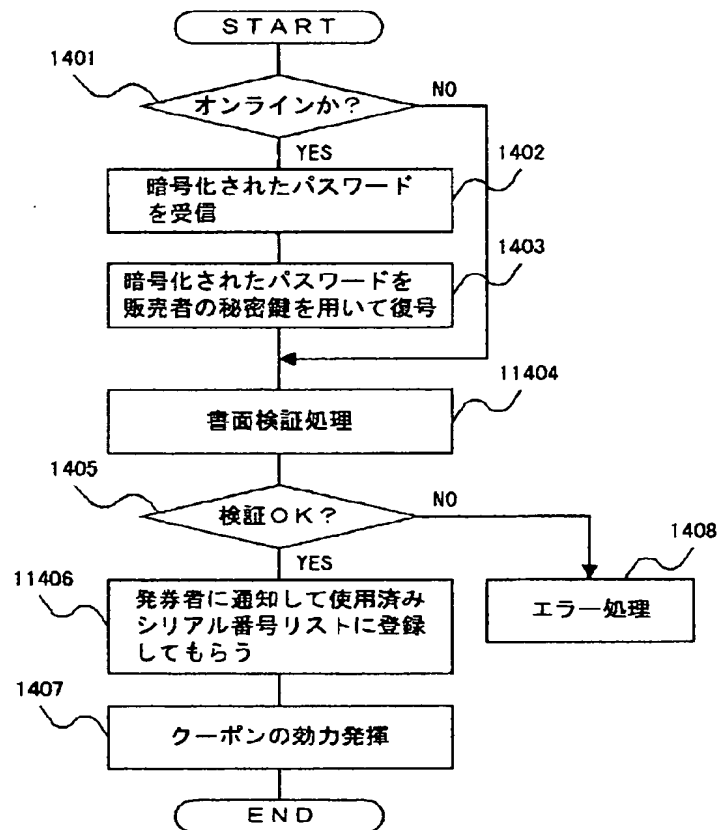
【図31】



【図32】

図 32

クーポン検証処理 (S6400)



33

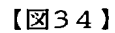
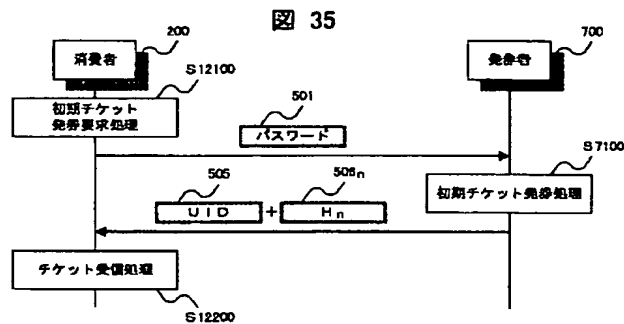
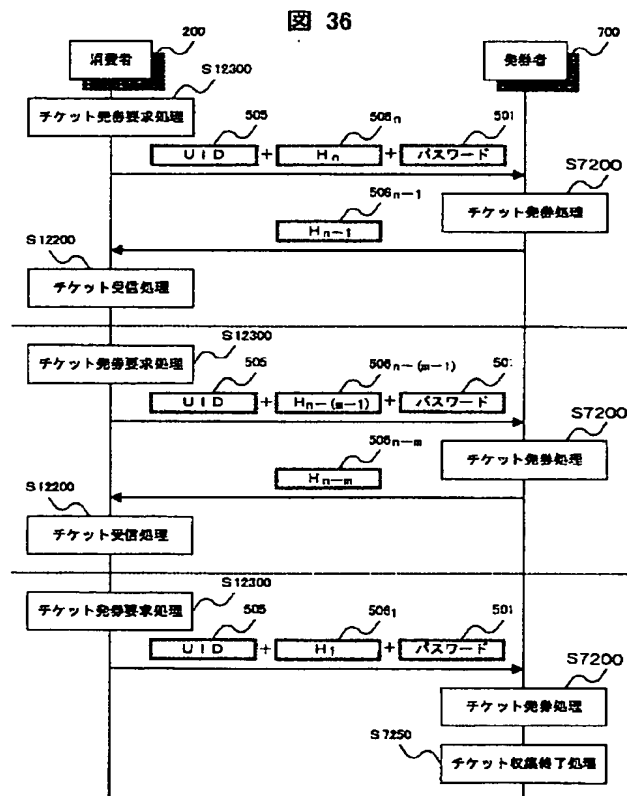


Figure 1 is a block diagram of a system architecture. A central horizontal bus, labeled 710バス, connects several components. Above the bus are three modules: 通信インターフェース (702), 表示装置 (703), and 入力装置 (704). Below the bus are three modules: 記憶装置 (705), CPU (706), and a large block labeled オペレーティングシステム (707a). The オペレーティングシステム block contains two sub-blocks: クーポン発行・検証処理プログラム (707b) and チケット発行・検証処理プログラム (707c). A 701発券音噴嘴 is connected to the top of the system. A 707メモリ block is connected to the bottom of the OS block.

【図35】



【図36】



フロントページの続き

(72)発明者 豊島 久
東京都江島区新砂一丁目6番27号 株式会
社日立製作所公共情報事業部内

(72)発明者 齋藤 司
東京都江島区新砂一丁目6番27号 株式会
社日立製作所公共情報事業部内